TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

AI and Algorithmic Recruitment Systems under EU Law

Compliance Complexity and Inadequate Protection

Henni Parviainen

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. B OSA – TOM. 772 | HUMANIORA | TURKU 2026

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

AI AND ALGORITHMIC RECRUITMENT SYSTEMS UNDER EU LAW

Compliance Complexity and Inadequate Protection

Henni Parviainen

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. B OSA – TOM. 772 | HUMANIORA | TURKU 2026

University of Turku

Faculty of Law
Employment Law, Data Protection Law
Doctoral Programme in Law

Supervised by

Professor Mika Viljanen
University of Turku
Turku, Finland

Associate Professor Annika Rosin
University of Turku
Turku, Finland

Reviewed by

Assistant Professor Marta Otto
University of Warsaw
Warsaw, Poland

Professor Ulla Liukkunen
University of Helsinki
Helsinki, Finland

Opponent

Assistant Professor Marta Otto
University of Warsaw
Warsaw, Poland

The originality of this publication has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

ISBN 978-952-02-0679-6 (PRINT)
ISBN 978-952-02-0680-2 (PDF)
ISSN 0082-6987 (Print)
ISSN 2343-3191 (Online)
Painosalama, Turku, Finland, 2026

UNIVERSITY OF TURKU
Faculty of Law
Employment Law, Data Protection Law
HENNI PARVIAINEN: AI and Algorithmic Recruitment Systems under EU Law – Compliance Complexity and Inadequate Protection
Doctoral Dissertation, 409 pp.
May 2026

ABSTRACT

The use of artificial intelligence (AI) and other algorithmic systems in recruitment may offer employers cost and efficiency benefits. However, the use of such algorithmic recruitment systems (ARS) introduces significant legal challenges and risks, particularly where ARSs support or automate decision-making. Despite increasing regulatory and scholarly attention, a comprehensive and systematic legal analysis of how EU legislation constrains and shapes the use of ARSs and protects job applicants from associated risks had not been conducted. This dissertation addresses that gap by examining two research questions.

First, this dissertation examines how EU legislation constrains and shapes employers' use of ARSs that involve AI and algorithmic decision-making. Second, it analyses what legal safeguards EU legislation provides to protect job applicants against data protection infringements and discrimination arising from the use of such ARSs, and assesses their adequacy. Drawing on the findings, I argue that despite the multiple constraints and conditions imposed on employers' use of ARSs, the EU-level legal framework is inadequate to protect job applicants from the risks posed by ARSs that involve AI or algorithmic decision-making. The inadequacy stems primarily from vague legal parameters, limited ex-ante oversight, structural barriers to enforcement by job applicants, and inherent limitations of available remedies.

This dissertation adopts a primarily legal dogmatic approach, interpreting and systematising relevant provisions across multiple EU legal instruments. This analysis produces a framework of key legal parameters for ARS use, categorising applicable norms into bans, obligations, specific duties and actionable rights.

The framework reveals that only a few specific ARS use cases are categorically banned, such as social scoring in AI-based recruitment systems. Most ARSs remain permissible but are subject to multiple vague legal parameters concerning data protection, non-discrimination and transparency. While the vaguely formulated legal parameters grant employers considerable leeway in deploying ARSs, they also create significant uncertainty, making it challenging for employers to ensure compliance with EU legislation. However, even if the legal parameters were clear, ensuring compliance could be difficult as the ARSs are complex and opaque, and employers may struggle to sufficiently understand and affect their workings to adhere to the legal parameters. These compliance difficulties pose risks to employers, as sanctions for non-compliance may be substantial.

However, under the current legal framework, there is no systematic ex-ante oversight of ARSs, which emphasises the role of ex-post enforcement. If supervisory

authorities do not have sufficient resources to investigate ARSs and enforce the legislation, the primary responsibility for detecting faults and breaches and making employers accountable for those falls on job applicants and the organisations representing them. Yet, the ex-post enforcement faces several obstacles. Due to the vague legal parameters and limited access to unmediated information about the ARSs, job applicants often lack the information needed to detect rights violations. Even when rights infringements are suspected, proving such allegations in judicial proceedings poses a further challenge. The modest probability of successful enforcement also weakens the deterrent effect of the legal parameters in practice, reducing employers' incentive to ensure compliance and leaving job applicants with limited assurance that the legal parameters will be observed.

Judicial interpretation of the existing legal framework could partially mitigate the problems job applicants face. Courts could, for instance, shift the burden of proof to the employer at a lower evidentiary threshold where the ARS used is opaque and technically complex. Such interpretations could also strengthen the preventive effects of the legislation by creating incentives for employers to deploy more transparent and compliant systems or, in extreme cases, to refrain from using certain ARSs altogether. The interpretative solutions, however, are contingent on applicants' ability to initiate proceedings in the first place and do not resolve the limitations of the available remedies. Even where a violation is successfully demonstrated, the available remedies may amount to only monetary compensation, while the loss of a job opportunity remains irreversible.

Taken together, these findings indicate that the EU's legal framework concerning the use of ARSs creates compliance challenges for employers and leaves job applicants insufficiently protected. While employers' compliance challenges could be alleviated by future case law and guidance from authorities, adequate protection for job applicants would require further legislative development. In the meantime, the framework of key legal parameters serves as a practical tool to help various stakeholders navigate the fragmented, constantly evolving regulatory environment surrounding ARSs.

KEYWORDS: AIA, artificial intelligence, algorithmic decision-making, algorithmic recruitment, data protection, EU law, GDPR, job applicants, non-discrimination, remedies

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta
Työoikeus, tietosuoja
HENNI PARVIAINEN: AI and Algorithmic Recruitment Systems under EU Law – Compliance Complexity and Inadequate Protection
Väitöskirja, 409 s.
Toukokuu 2026

TIIVISTELMÄ

Tekoälyn (AI) ja muiden algoritmisten järjestelmien käyttö rekrytoinnissa voi tarjota työnantajille kustannus- ja tehokkuushyötyjä. Tällaisten algoritmisten rekrytointijärjestelmien (ARS) käyttö tuo kuitenkin mukanaan merkittäviä oikeudellisia haasteita ja riskejä erityisesti silloin, kun järjestelmät tukevat tai automatisoivat päätöksentekoa. Sääntelyssä ja tutkimuksessa on enenevissä määrin kiinnitetty huomiota ARS:iin. Kattavaa ja systemaattista oikeudellista analyysiä siitä, miten EU:n lainsäädäntö rajoittaa ja ohjaa ARS:ien käyttöä sekä suojaa työnhakijoita niihin liittyviltä riskeiltä ei ollut kuitenkaan toteutettu. Tämä väitöskirja vastaa kyseiseen tutkimusaukkoon tarkastelemalla kahta tutkimuskysymystä.

Ensinnäkin tässä väitöskirjassa tutkitaan, miten EU:n lainsäädäntö rajoittaa ja muovaa työnantajien mahdollisuuksia käyttää ARS:iä, joihin sisältyy tekoälyä ja algoritmista päätöksentekoa. Toiseksi väitöskirjassa analysoidaan, mitä oikeudellisia suojamekanismeja EU:n lainsäädäntö tarjoaa työnhakijoille tällaisten ARS:ien käytöstä aiheutuvia tietosuojaloukkauksia ja syrjintää vastaan sekä arvioidaan näiden suojamekanismien riittävyyttä. Näiden kysymysten analyysi kiteytyy väitöskirjan keskeiseen argumenttiin: huolimatta lukuisista rajoituksista ja ehdoista, joita työnantajien ARS:ien käyttöön kohdistuu, EU:n voimassa oleva sääntelykehys ei riitä suojelemaan työnhakijoita ARS:ien aiheuttamilta riskeiltä. Riittämättömyys aiheutuu ensisijaisesti epätarkasti määritellyistä oikeudellisista parametreista, rajallisesta ennakkovalvonnasta, työnhakijoiden kohtaamista rakenteellisista esteistä oikeuksiensa käyttämiselle ja täytäntöönpanolle sekä käytettävissä olevien oikeussuojakeinojen sisäänrakennetuista rajoituksista.

Väitöskirjassa sovelletaan ensisijaisesti lainopillista tutkimusmenetelmää tulkitsemalla ja systematisoimalla useita EU-oikeudellisia säädöksiä. Analyysin tuloksena muodostetaan ARS:ien käyttöön sovellettavien oikeudellisten parametrien kehikko, joka luokittelee sovellettavat normit kieltoihin, velvollisuuksiin, erityisiin velvoitteisiin ja vetoamista edellyttäviin oikeuksiin.

Oikeudellisten parametrien kehikko osoittaa, että vain harva ARS:ien käyttötapaus on ehdottomasti kielletty, kuten sosiaalinen pisteytys tekoälypohjaisissa rekrytointijärjestelmissä. Suurta osaa ARS:istä on sallittua käyttää. Kaikkien ARS:ien käyttö edellyttää kuitenkin useiden erityisesti tietosuojaan, syrjinnän kieltoon ja läpinäkyvyyteen tähtäävien monitulkintaisten oikeudellisten parametrien noudattamista. Epätarkasti muotoillut oikeudelliset parametrit jättävät työnantajille liikkumavaraa ARS:ien käyttöönotossa, mutta samalla ne luovat merkittävää epävarmuutta ja vaikeuttavat työnantajien mahdollisuuksia varmistaa, että ne

noudattavat sääntelyä. Vaikka oikeudelliset parametrit olisivat selkeät, ARS:ien monimutkaisuus ja läpinäkymättömyys vaikeuttavat lainsäädännön noudattamisen varmistamista, sillä työnantajat eivät välttämättä ymmärrä järjestelmiä ja pysty vaikuttamaan niiden toimintaan riitävästi. Nämä sääntelyn noudattamisen haasteet luovat työnantajille riskejä, sillä seuraamukset vaatimusten laiminlyönnistä voivat olla huomattavia.

Voimassa oleva EU:n sääntelykehys ei edellytä ARS:ien systemaattista ennakkovalvontaa, mikä korostaa jälkikäteisen oikeusturvan ja täytäntöönpanon merkitystä. Jos valvontaviranomaisilla ei ole riittäviä resursseja ARS:ien tutkimiseen ja lainsäädännön täytäntöönpanoon, ensisijainen vastuu puutteiden ja rikkomusten havaitsemisesta sekä työnantajien saattamisesta vastuuseen niistä jää työnhakijoiden ja heitä edustavien organisaatioiden harteille. Jälkikäteiseen oikeusturvaan ja täytäntöönpanoon kohdistuu kuitenkin useita ongelmia. Epätarkkojen oikeudellisten parametrien ja ARS:iä koskevan välittömän ja suodattamattoman tiedonsaannin rajallisuuden vuoksi työnhakijoilla ei usein ole riittävästi tietoa oikeuksiensa loukkausten havaitsemiseksi. Silloinkin, kun oikeuksia epäillään loukatun, väitteiden todistaminen tuomioistuinmenettelyssä on vaikeaa. Täytäntöönpanon onnistumisen alhainen todennäköisyys heikentää käytännössä myös oikeudellisten parametrien ennaltaehkäisevää vaikutusta ja vähentää työnantajien kannustimia varmistaa, että ne noudattavat säädöksiä. Nämä seikat lisäävät myös työnhakijoiden epävarmuutta siitä, noudatetaanko oikeudellisia parametreja.

Lainsäädännön tulkinnalla tuomioistuimissa voitaisiin osittain lieventää työnhakijoiden kohtaamia ongelmia. Tuomioistuimet voisivat esimerkiksi siirtää todistustaakan työnantajalle alhaisemmalla näyttökynnyksellä, jos käytetty ARS on läpinäkymätön ja teknisesti monimutkainen. Tällaiset tulkinnat voisivat myös vahvistaa lainsäädännön ennaltaehkäiseviä vaikutuksia luomalla työnantajille kannustimia ottaa käyttöön läpinäkyvämpiä ja lainsäädännön vaatimukset paremmin täyttäviä järjestelmiä. Äärimmäisissä tapauksissa tulkinnat saattaisivat jopa kannustaa pidättäytymään joidenkin ARS:ien käytöstä kokonaan. Tuomioistuinten tulkintaratkaisut auttavat kuitenkin vain siinä tapauksessa, että työnhakijat vievät asiansa oikeuteen, eivätkä ne ratkaise käytettävissä olevien oikeussuojakeinojen rajoituksia. Vaikka työnhakijat menestyisivät oikeudenkäynnissä, he olisivat EU-oikeuden nojalla oikeutettuja ainoastaan rahalliseen korvaukseen. Työtilaisuuden työnhakijat menettävät peruuttamattomasti.

Yhdessä nämä havainnot osoittavat, että työnantajat kohtaavat merkittäviä haasteita ARS:ien käyttöä koskevan EU:n voimassa olevan sääntelykehyksen noudattamisessa, eikä sääntelykehys suojaa riittävästi työnhakijoita. Työnantajien taakkaa voisivat helpottaa tuleva oikeuskäytäntö ja viranomaisten ohjaus; työnhakijoiden riittävän suojan takaaminen sen sijaan edellyttäisi lainsäädännöllisiä muutoksia. Näitä kehitysaskeleita odotellessa tässä väitöskirjassa kehitetty oikeudellisten parametrien kehikko voi auttaa eri sidosryhmiä hahmottamaan ARS:ien käyttöä ohjaavaa pirstaleista ja jatkuvasti muuttuvaa sääntelyä.

AVAINSANAT: tekoälysäädös, tekoäly, algoritminen päätöksenteko, algoritminen rekrytointi, tietosuoja, EU-oikeus, yleinen tietosuoja-asetus, työnhakijat, syrjintäkielto, oikeussuojakeinot

Acknowledgements

Writing a dissertation was a long-standing, distant aspiration, something I imagined pursuing far in the future. When I encountered algorithmic workforce management systems and realised their legal implications, I knew it was the topic I wanted to dig into. However, to keep up with the rapidly evolving topic, the project could not be postponed. Embarking on this study and writing this dissertation would not have been possible without the support of many people and institutions, to whom I now wish to express my sincere gratitude.

First of all, I would like to thank my supervisors, Professor Mika Viljanen and Associate Professor Annika Rosin, an ideal combination of supervisors for a project of this nature. I am profoundly grateful for all the time Annika and Mika have invested in this project, as well as their invaluable guidance, support and encouragement throughout. The opportunity to work on their projects also provided essential financial support at critical stages of this dissertation. Beyond these contributions, I have learned much of what I know about academic writing from Annika and Mika, and it has been a privilege to co-write with both of them. Substantively, Mika's extensive knowledge of both law and technology has been highly valuable, while Annika has generously shared her profound expertise in EU labour law. Their constructive and insightful comments on the article drafts and this synthesis have significantly improved the text.

I am also grateful to the pre-examiners, Professor Ulla Liukkunen and Assistant Professor Marta Otto, for taking the time to read the lengthy manuscript and for providing their constructive feedback, which helped me to make the final improvements to this dissertation. I am particularly honoured that Assistant Professor Marta Otto has also kindly agreed to serve as my opponent at the public defence.

Several other pairs of eyes have also reviewed my texts and provided valuable feedback. I am thankful to all the anonymous reviewers of the original publications. Likewise, I am grateful for the comments I received in the Faculty's dissertation seminars from both fellow doctoral researchers and the professors who chaired the seminars.

I am profoundly grateful to all my colleagues at the Faculty of Law; it is an honour to be part of this community. Over the years, several illuminating discussions in the coffee room and at faculty events have supported this project in various ways. Special thanks to all fellow Doctoral Researchers for their peer support, and to colleagues at more senior stages of their careers for sharing their experience of the dissertation process and academic work more broadly. I am also grateful for the opportunity to serve on the Research Committee, an experience that has broadened my understanding of the Faculty's academic work.

The regular meetings and discussions with Juho Aalto were especially valuable when writing this synthesis. Having someone in a similar situation, from whom to ask the less obvious questions and with whom to share both frustration and progress, was genuinely important. I have also greatly enjoyed collaborating and exchanging ideas with Sini Mickelsson and Nea Lepinkäinen, whose expertise in data protection and privacy, and AI regulation respectively, has enriched many discussions along the way. Over the years, I have had the pleasure of sharing an office with several colleagues. Most recently, Sonja Vilenius and Lauri Salonen have been my roommates, whose company has made the working days in Calonia all the more enjoyable.

Special thanks are also due to my administrative supervisors Professor Mika Viljanen, Associate Professor Daniela Alaattinoglu and Associate Professor Mikko Rajavuori, for their encouraging and helpful support. Professor Teemu Juutilainen and Professor Emerita Anne Kumpula served as members of the steering group for this project and provided valuable oversight, ensuring the project continued to move forward. On the practical side, I am also grateful to the Coordinator of the Doctoral Programme Kirsi Tuohela, and the former Coordinator Mirkka Ruotsalainen, for their kind and patient guidance in administrative matters throughout my doctoral studies. Thanks are also due to Gerda Volt for her kind assistance with the practical arrangements of the defence. Further, I wish to thank Research Assistant Sara Ylimäki for her careful proofreading of parts of this synthesis and Research Assistant Jonas Lund for checking the lists prior to pre-examination.

I am also grateful for having had the opportunity to present my research at conferences to external audiences. The comments received and the discussions had in the conferences have enriched my thinking. I am therefore thankful to the participants in the Digital Technology Regulation Colloquium 2024 at the University of Helsinki, the Doctoral Panel at the XXXIX Nordic Conference on Law and IT 2024 at Stockholm University, the WORK2025 conference at the University of Turku, and the EC2U PhD Network Meeting 2025 at the University of Jena. While finalising this dissertation, I also had the opportunity to attend the 4th conference of the Nordic Network of Labour Law Scholars at the University of Southern Denmark,

where the supportive atmosphere provided welcome encouragement in the final stages.

I am truly grateful for the financial support for this dissertation and related travels provided by the Eino Jutikkala Fund of the Finnish Academy of Science and Letters, the University of Turku, the Foundation of the 25th March, the Heldt Stipend Foundation and the University of Turku Research Grant Fund. In addition to personal grants, I have had the privilege of working on several projects funded by the Research Council of Finland, namely AMEMPLOY, AALAW and ETAIROS, as well as on the AIGA project funded by Business Finland.

Beyond the academic community, the support of the people closest to me has been invaluable. I am deeply grateful to my parents, who have always encouraged me to pursue what I truly enjoy and supported me in every possible way. Without their love and encouragement, this dissertation would never have come into existence. Kiitos kaikesta äiti ja isä! Special thanks also to my aunt Paula, who helped track down sources throughout my studies, ensuring that many which would otherwise have gone unfound ended up on these pages. Many other family members have also offered invaluable help during this project, whether by taking care of the children when I had to finalise a publication or returning my books to various Finnish libraries. I am also grateful to my friends for their encouragement and for providing a welcome balance to the academic work, whether on the running trail, hiking path or the playground.

I owe my warmest gratitude to my spouse, Antti, whose calm and positive outlook has provided both encouragement and an environment where pursuing one's aspirations feels achievable. I am also grateful to Antti for keeping the house standing and the children happy at the busiest times. This project at times encroached on family time, and I am thankful for the patience and understanding with which that was borne. Finally, I am sincerely grateful to Eelis and Ellen for keeping things in perspective and reminding me what is truly important in life. Their smiles, laughter, hugs, play and chatter are a source of joy I dearly cherish.

Lieto, April 25, 2026

Henni Parviainen

Table of Contents

Tables

Figures

List of Original Publications

This dissertation is based on the following original publications, which are referred to in the text by their Roman numerals:

I Mika Viljanen & Henni Parviainen. AI Applications and Regulation: Mapping the Regulatory Strata. *Frontiers in Computer Science*, 2022; 3:779957: 1-11.

II Henni Parviainen. Can algorithmic recruitment systems lawfully utilise automated decision-making in the EU? *European Labour Law Journal*, 2022; 13(2): 225-248.

III Henni Parviainen. Challenges of Direct Discrimination in Algorithmic Recruitment – Insuperable or Not? *International Journal of Comparative Labour Law and Industrial Relations*, 2024; 40(4): 437-466.

IV Henni Parviainen. Effective remedies for job applicants in algorithmic recruitment: the contribution of the EU Artificial Intelligence Act. *Law, Innovation and Technology (accepted for publication in Vol 18(2), 2026).*

1 Introduction

1.1 Artificial intelligence and algorithmic systems in recruitment: the case for legal analysis

1.1.1 Perceived promises, risks and regulatory context

Employers increasingly utilise artificial intelligence (AI) and other algorithmic systems across various tasks, including recruitment.[1] According to European Employment Services, 70% of European human resources professionals use AI-based tools in their recruitment processes.[2] Numerous AI and other algorithmic systems designed for recruitment claim to assist human recruiters or automate specific stages of the recruitment process.[3] Such systems are collectively referred to here as *algorithmic recruitment systems (ARSs),* and their deployment is referred to as *algorithmic recruitment.*[4] ARSs may be deployed across multiple stages of recruitment, including sourcing candidates, screening applications, conducting

1 See, e.g., (Fabris et al. 2024, 1–2; Larsson et al. 2024, 8–10; Milanez et al. 2025, 20). Recruitment processes have generated vast amounts of data for years, making recruitment a promising use case for AI (De Stefano and Wouters 2022, 10; Ball 2010, 91).

2 (European Employment Services 2024). Precise data on the adoption of AI in recruitment processes across the EU seems to be scarce. The EURES refers to data published in 2023 by UNLEASH, a global digital media and events business (UNLEASH 2023). Upon closer examination, the data appears to refer to the use of AI tools within human resources (HR) processes in general, rather than specifically in recruitment. As *Stefan Larsson et al.* found in their study of major Swedish employers, the uptake of AI can be difficult to measure, as employers might not realise that the digital platforms they use also utilise AI or algorithmic decision-making (Larsson et al. 2024, 13).

3 (Fabris et al. 2024, 3). However, general-purpose AI systems, such as large language models (LLMs), can also be deployed in recruitment contexts without recruitment-specific adaptations, see, e.g., (Alba and Yin 2024).

4 However, where it is necessary for analytical purposes to differentiate between AI and other algorithmic systems, I will use those terms separately. For the definition of an algorithmic recruitment system, see section 2.4, and for the key characteristics of such systems, see Chapter 3 below.

interviews, and supporting final selection decisions.[5] Some ARSs merely assist human recruiters with recruitment-related tasks, such as drafting general job descriptions or advertisements,[6] while others support or automate decision-making concerning individual job applicants.[7] Such decision-making support and automation are collectively referred to here as *algorithmic decision-making*.[8] Although all ARSs raise legal concerns, algorithmic decision-making poses heightened risks to individual job applicants, as the decisions often have irreversible consequences.[9]

Nevertheless, proponents argue that ARSs can fast-track recruitment, enhance accuracy, consistency, and quality, reduce bias, decrease human recruiters' workload, and lower costs.[10] These promises make ARSs an appealing choice for employers. AI adoption in recruitment, however, is not limited to employers. Some reports suggest that in certain European countries, and at least within specific sectors, a significant proportion of job applicants also utilise AI in their job search.[11] Job applicants' use of AI may increase application volumes, which in turn creates additional pressure on employers to implement ARSs to process the applications.[12]

Yet, algorithmic recruitment reshapes how talent is identified, evaluated, engaged, and excluded.[13] These changes have profound implications for both individual job applicants and society, influencing access to employment, financial stability, opportunities for participation in society, and the development of personal

5 See, e.g., (Fabris et al. 2024, 3–4; Black and van Esch 2020, 218–22; Bogen and Rieke 2018, 13–43). See section 3.1 below for a more detailed discussion on the ARS use cases.

6 However, this stage may also significantly affect the applicant pool, see, e.g., (Black and van Esch 2020, 19; Bogen and Rieke 2018, 15–19).

7 See, e.g., (Graham et al. 2020, 23; Centre for Data Ethics and Innovation 2021, 47; Gavaghan et al. 2021, 46–47; Bogen and Rieke 2018, 13).

8 See section 2.3 below for a more detailed definition.

9 Prior studies suggest that, particularly, the rejections are often automated, see, e.g., (Centre for Data Ethics and Innovation 2021, 47; Gavaghan et al. 2021, 47; Bogen and Rieke 2018, 13).

10 See, e.g., (Horodyski 2023, 7; Cappelli et al. 2023, 8; Broecke 2023, 27–33; Bornstein 2018, 532–33; Fabris et al. 2024, 37; Houser 2019, 325–30).

11 Numbers vary considerably across countries and sectors. For instance, in early 2024, it was estimated that about half of the applicants in the UK already used generative AI (Criddle and Strauss 2024). In a French survey, it was found that more than 75% of workers had used AI in their job search (Duboust 2025). By contrast, a Finnish survey from 2024 found that only 16% of job applicants reported using AI (Duunitori 2024, 18).

12 (Lacková 2022, 72).

13 See also (Köchling and Wehner 2020, 830–35; Leicht-Deobald et al. 2019, 381–86; Ajunwa 2020, 1683–92) and section 3.1 below.

identity.[14] Recruitment inherently involves processing personal data to assess applicants' suitability and make hiring decisions, which also carries the potential for bias or discrimination. While the long-term effects of algorithmic recruitment remain unknown, there is growing evidence that, through their increased technical complexity, operational scale and opacity, particularly systems involving AI and algorithmic decision-making may pose threats to job applicants' fundamental rights.[15]

Accordingly, algorithmic recruitment may, among other problems, amplify the existing risks of data protection breaches and discriminatory outcomes.[16] First, the ARSs' technical complexity and capacity to process large volumes of personal data may, for instance, enable subtle inferences that possibly involve special category personal data[17] and exacerbate information asymmetries between employers and job applicants.[18] Moreover, those capabilities may increase the risk of processing unnecessary or inaccurate personal data[19] and of suffering data breaches that expose personal data.[20] Further, the simplicity of automated decision-making may increase its use even in the absence of a lawful basis. Together, these issues create considerable risks to job applicants' right to protection of personal data as guaranteed under Article 8 of the Charter of Fundamental Rights of the European Union (CFREU).[21] Second, ARSs can replicate the human biases embedded in their training data, potentially resulting in systemic and enduring discriminatory practices that breach job applicants' right to non-discrimination as protected under CFREU Article

14 See, e.g., (Rigotti and Fosch-Villaronga 2024, 1; Sánchez-Monedero et al. 2020, 2–3).

15 See, e.g., (Rigotti and Fosch-Villaronga 2024, 3; Parodi 2024, 122; Capasso et al. 2025; Giermindl et al. 2022, 414, 418, 423–24; Grozdanovski 2021, 100–101; Kelly-Lyth 2021, 902–5; Martínez Ramil 2021; Köchling and Wehner 2020; Raso et al. 2018, 42–46). Of the fundamental rights impacts of AI and algorithmic decision-making in general, see, e.g., (European Union Agency for Fundamental Rights 2020; Teo 2023, 217–19; Risse 2019, 11–15).

16 For practical examples, see section 3.1 below.

17 See, e.g., (ICO 2024, 22; Kelly-Lyth 2021, 912–13).

18 See, e.g., (Sánchez-Monedero et al. 2020, 3; Lacková 2022, 89–90).

19 For instance, LLMs have an inherent feature of producing confabulations (Smith et al. 2023), i.e. hallucinations, meaning seemingly plausible but nonfactual content or content that diverges from input data, see (Huang et al. 2024, 2; OECD 2023, 10; Novelli et al. 2024, 13). The confabulations could also concern individual job applicants, amounting to inaccurate personal data (Engel et al. 2023, 3).

20 (Carlini et al. 2023; EDPB 2024b, 18; OECD 2023, 30 and 34; Weidinger et al. 2022, 217–18).

21 Particularly, the subtle inferences involving special category data, information asymmetries and data breaches, also implicate job applicants' right to privacy under CFREU Art. 7. However, a full analysis of privacy implications falls outside the scope of this dissertation.

21.[22] Since ARSs operate at a scale far exceeding that of individual human recruiters, the potential for harm is amplified far beyond what a biased or careless human recruiter could cause.[23] For instance, a single biased ARS can quickly have widespread consequences for the labour market by systematically excluding certain applicant groups.[24] Third, the opacity of ARSs, combined with job applicants' limited access to information about how the systems function, makes it difficult for applicants to understand and challenge decisions that appear unlawful.[25] These obstacles could undermine job applicants' ability to hold employers accountable for non-compliant ARS deployment and threaten their right to an effective remedy as guaranteed in CFREU Article 47.[26]

The risks associated with AI and algorithmic decision-making may be particularly severe for job applicants, who can be even more vulnerable than employees due to factors such as job insecurity, financial pressure stemming from unemployment, constrained professional networks and limited support from trade unions. This vulnerability is not comprehensively addressed by EU labour law, as most EU labour legislation protects only subordinate employees as the weaker party in the employment relationship, and does not apply before the employment relationship begins.[27] Consequently, EU labour legislation does not, for instance, provide job applicants with rights to information regarding the recruitment

22 This could risk breaching also the job applicants' rights to equality (CFREU Art. 23). Of these risks, see e.g., (Kim 2017, 886–90; Bogen and Rieke 2018, 8; Hacker et al. 2023, 1113; Luccioni and Viviano 2021; Barocas and Selbst 2016, 677–93; Gerards and Xenidis 2020, 43; Kelly-Lyth 2021, 903; Ajunwa 2023, 84).

23 See, e.g., (Ajunwa 2023, 80; De Stefano and Wouters 2022, 11 and 32; Alexander III et al. 2025, 4; Gerards and Xenidis 2020, 46).

24 See also (De Stefano and Wouters 2022, 11). With LLM-based recruitment systems, this risk is exacerbated, as the same biased LLM could be used as a basis for several different ARSs, see also (Bommasani et al. 2021, 1 and 5).

25 Of these risks, see, e.g., (Hunkenschroer and Luetge 2022, 997; Kelly-Lyth 2021, 904; Grozdanovski 2021, 127; Gerards and Xenidis 2020, 45; Houser 2019, 340–41; Pasquale 2015, 3). However, human decision-making is opaque as well, see, (Nisbett and DeCamp Wilson 1977; Kleinberg et al. 2018, 116).

26 See, e.g., (European Union Agency for Fundamental Rights 2020, 13). Yet, recruitment is one context in which algorithmic decision-making systems have already been challenged in practice (Barros Vale and Zanfir-Fortuna 2022, 39–41).

27 On this traditional focus of labour laws, see, e.g., (Davidov 2017, 374; Weiss 2011, 48; Davidov 2016b, 119; Hendrickx 2018, 200; Gramano 2024). Discussions on broadening the scope of labour law to include self-employed workers have persisted for years, see, e.g., (Kountouris 2018; Weiss 2011, 48; Bercusson 2009, 370; Menegatti 2020). *Eva Lacková* has also noted the pre-employment stage, considering that the lack of subordination alone does not indicate that job applicants would not require protection by labour laws (Lacková 2022, 71–75).

processes, which exacerbates the informational asymmetries.[28] The gap left by EU labour legislation is partially addressed by the general EU-level legislation that regulates the use of ARSs, regardless of employment status.

The primary legislative instruments addressing the risks caused by algorithmic recruitment are the General Data Protection Regulation (GDPR)[29], the Artificial Intelligence Act (AIA)[30], and the Non-Discrimination Directives[31]. The CFREU also protects job applicants from the risks of ARSs.[32] Together, these EU-level instruments establish the minimum level of protection for job applicants across Member States that all use of ARSs in the EU must satisfy.[33] Uncertainty regarding these instruments, particularly the constraints they impose on algorithmic recruitment and the protection they provide to job applicants, motivated this dissertation.

28 For instance, the Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community - Joint declaration of the European Parliament, the Council and the Commission on employee representation (hereinafter 'Information and Consultation Directive') does not provide job applicants with any rights to information and consultation or representation in such proceedings.

29 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

30 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

31 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (Race Equality Directive, hereinafter RED), Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation (Employment Equality Directive, hereinafter EED) and Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) (Gender Equality Directive, hereinafter GED). Hereinafter, these three directives applicable in the recruitment context are referred to as 'Non-Discrimination Directives'.

32 See, e.g., CFREU Arts. 8, 21 and 47. See section 1.3.2 below for a more detailed discussion on the effects of fundamental rights in the algorithmic recruitment context.

33 Treaty on the Functioning of the European Union (TFEU) Art. 288.

1.1.2 Gaps in legal scholarship

At the outset of this dissertation project, legal scholarship addressing algorithmic recruitment from the perspective of EU legislation was sparse.[34] Over the course of the project, the topic has attracted growing scholarly attention, and EU-focused studies have since appeared more frequently in the literature.[35] Yet the technological and regulatory landscape has shifted notably, generating questions that existing scholarship has not yet addressed.

First, the ARSs used have advanced considerably over the past few years, as the adoption of general-purpose AI (GPAI)[36], such as large language models (LLMs)[37] and generative AI[38] systems, has increased.[39] At a general level, legal scholarship has started to explore how existing regulations address the latest developments in AI.[40] Prior studies suggest that the use of LLMs could, for instance, affect the effectiveness of bias mitigation measures, which are particularly important in the recruitment context.[41] However, there is limited scholarship on how recent technical developments affect the constraints that EU legislation sets, especially for recruitment systems involving AI.[42] While legal scholarship is still grappling with the implications of GPAI systems, technological

34 See (Kullmann 2019) and more broadly from the perspective of workforce analytics, see (Otto 2018). From the US perspective, see (Kim 2017; Houser 2019; Mainka 2019).

35 See, e.g., (Carter 2024; Rigotti and Fosch-Villaronga 2024; Parodi 2024; Hunkenschroer and Kriebitz 2023; Kelly-Lyth 2021; Grozdanovski 2021).

36 General-purpose AI systems refer to systems that can be used for a variety of purposes, both directly and as integrated into other AI systems. See AIA Art. 3, point 66.

37 LLMs are 'text-generation engines' trained on a vast corpus of text 'to predict which string of words comes next in a piece of text' (Wachter et al. 2024, 2). See section 3.3.2 for a more detailed discussion on LLMs.

38 Generative AI refers to AI algorithms and models that can produce novel and meaningful content (e.g., text, images, video, or audio) based on training data, see (Feuerriegel et al. 2024, 111; He et al. 2025, 1).

39 See, e.g., (Bick et al. 2024; Alba and Yin 2024; Srinivasan 2024; Criddle and Strauss 2024; Chaudhary 2023; Rathnayake and Gunawardana 2023).

40 See, e.g., (Hacker et al. 2025; Ohm 2024; Hacker et al. 2023). The authorities have also only started to address the 'systemic, abstract and novel issues' the AI models raise, for instance, in the context of the GDPR (EDPB 2024b, 8–9). See also (EDPB 2024c).

41 See, e.g., (Ohm 2024, 216–17).

42 See (Publication III / Parviainen 2024).

development continues at a rapid pace,[43] and the first wave of agentic AI[44] has already reached the recruitment field.[45]

Second, the regulatory landscape has also evolved with the entry into force of the AIA on 1st August 2024,[46] raising numerous questions regarding its practical application in the recruitment context. For instance, the AIA's ambiguous definition of AI systems[47] and classification of high-risk AI systems[48] create interpretative uncertainty, making it challenging to identify the constraints applicable to each AI recruitment use case. Legal scholarship plays a vital role in ensuring clarity in the interpretations and practical application of these new normative requirements.[49] Yet, so far, legal scholars have only briefly addressed what the AIA implies for the use of AI in recruitment.[50]

Overall, a comprehensive analysis and systematisation of the legal requirements set for using ARSs appears to be missing. The recruitment context is often incorporated into broader discussions on AI use in employment,[51] which risks overlooking the job applicants' particularly vulnerable position.[52] While writing this dissertation, recruitment-specific questions about AI and other algorithmic systems have been increasingly addressed in prior research, but typically in a selective manner, focusing on specific issues, such as discrimination,[53] data protection[54] and

43 The law's struggle to keep up with technological change is a broader issue, not limited only to AI. See, e.g., (Moses 2007; 2013).

44 Agentic AI refers to AI systems that can pursue open-ended objectives in complex environments by taking sequences of actions without human intervention, see (Watson 2025; Stryker 2025; Borrelli et al. 2025, 7). See section 3.3.3 below.

45 See, e.g., (Kshetri 2025; Bhattacharya and Verbert 2025; Andrews 2025; Abraham 2025).

46 Subsequently, the Council of Europe (COE) Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law also entered into force on 1st January 2025. For an analysis of the Convention, see e.g., (Chang 2024).

47 See AIA Art. 3, point 1. See also section 2.2 below and (Publication IV / Parviainen 2026).

48 AIA Art. 6. See also section 2.2 below and (Publication IV / Parviainen 2026).

49 (Celeste and Nair 2024, 1).

50 (Carter 2024, 353–56; Grozdanovski 2025). For an analysis of the AIA's effects on employment in general, see (Cristofolini 2024) and on AI fairness in hiring, see (Rigotti and Fosch-Villaronga 2024, 7).

51 See, e.g., (Adams-Prassl, Abraha, et al. 2023; Aloisi 2024; Kelly-Lyth 2023; Cristofolini 2024; Abraha 2023).

52 In general, the context of use has a significant impact on the effects of AI and algorithmic decision-making, see, e.g. (Smuha 2021, 65). This also highlights the need to consider the recruitment phase independently from the broader employment context.

53 See, e.g., (Grozdanovski 2021; 2025; Parodi 2024; Carter 2024; Greif and Grosz 2023; Martínez-Ramil 2022; Tilmes 2022; Kelly-Lyth 2021; Kullmann 2019). From the United States' perspective, see also (Barocas and Selbst 2016; Kim 2017).

54 See, e.g., (Lacková 2022; Kelly-Lyth 2021; Parodi 2024).

the possibilities for challenging decisions[55] or specific combinations of these. However, an integrated analysis of how the relevant EU legislative instruments collectively constrain and shape ARS use and protect job applicants from the risks of ARSs appears absent from the literature.

The existing scholarship closest to this dissertation's scope illustrates this gap. For instance, *Ljupcho Grozdanovski* and *Christine Carter* have both independently examined the problems of proving discrimination in algorithmic recruitment and have also identified the GDPR as a possible mechanism for accessing evidence.[56] Both have also analysed the potential role of the AIA in accessing evidence of algorithmic recruitment discrimination.[57] However, neither undertakes a comprehensive analysis of the full regulatory framework. Further, *Carlotta Rigotti and Eduard Fosch-Villaronga* have also briefly analysed data protection, non-discrimination, and AI legislation in the context of AI recruitment, particularly from a fairness perspective.[58] Nevertheless, their succinct examination of the legal framework appears to serve only a secondary role in their broader cross-disciplinary analysis.[59] In the UK context, *Aislinn Kelly-Lyth* has undertaken a more comprehensive analysis of the effectiveness of EU-derived data protection and non-discrimination laws regulating algorithmic recruitment, considering various constraints and protections.[60] Yet Kelly-Lyth's analysis is not strictly an EU law analysis given the UK's post-Brexit position, and it predates the AIA. Further, as an example of a more detailed study, *Elisa Parodi* has analysed the role of the GDPR in litigating discriminatory targeted job advertisements.[61] Apart from *Eva Lacková*'s data protection and labour law-focused paper on the fragility of pre-contractual relations in the context of algorithmic recruitment,[62] the limited protection offered to job applicants under EU labour law receives little explicit attention in the literature.

The following subchapter explains how this dissertation addresses these gaps.

55 See, e.g., (Kelly-Lyth 2021; Grozdanovski 2021; 2025; Carter 2024).
56 (Grozdanovski 2021; Carter 2024).
57 (Carter 2024, 353–56; Grozdanovski 2025, 11–20).
58 (Rigotti and Fosch-Villaronga 2024, 4–7).
59 (Rigotti and Fosch-Villaronga 2024).
60 (Kelly-Lyth 2021).
61 (Parodi 2024).
62 See (Lacková 2022, 71–75).

1.2 Objectives, research questions and central thesis

This dissertation examines EU-level legislation governing algorithmic recruitment from two perspectives: that of employers utilising ARSs and that of job applicants being subjected to them. The analysis focuses specifically on ARSs that involve AI or algorithmic decision-making, while remaining attentive to the broader algorithmic recruitment context.[63] As regards EU legislation, this dissertation examines binding legal norms that constrain and shape the use of ARSs, referred to throughout this dissertation as *legal parameters*.[64]

Building on the gaps identified in section 1.1.2, this dissertation pursues two interconnected aims. The first aim is to produce a comprehensive and systematised account of how EU legislation constrains and shapes employers' use of ARSs.[65] The second aim is to examine the existing EU-level safeguards for job applicants and to evaluate whether those are structurally adequate to protect job applicants against data protection infringements and discrimination arising from ARS use.

Several practical objectives complement these scholarly aims. This dissertation aims to support employers' compliance efforts when using ARSs.[66] It may also assist other ARS users, such as recruitment agencies, and ARS developers in ensuring adherence to legislation. Equally, this dissertation seeks to assist affected job applicants and their representatives in understanding and enforcing job applicants' rights under EU legislation. Moreover, it could support courts and authorities in enforcing the relevant EU legislation in the recruitment context.

In pursuit of these aims, this dissertation examines the following research questions:

63 See, e.g., Chapter 5 and the framework of key legal parameters for ARS use in *Annex I*, which covers the use of all kinds of ARSs, encompassing the whole algorithmic recruitment context.

64 The term *parameter* reflects the boundary-setting function of law, while situating legal constraints within a broader set of constraints that includes also technical and organisational parameters shaping the use of ARSs (see sections 3.3–3.4 below). The term *legal parameter* has been used in prior legal scholarship, although in another field of law, see, e.g., (Williams et al. 2004). See also (Albin 2025, 97) referring specifically to 'parameters governing the use of employees' personal data'.

65 For instance, *Edoardo Celeste and Abhilash Nair* have highlighted the importance of legal scholarship in ensuring that the novel 'normative requirements are clearly interpreted and effectively implemented'(Celeste and Nair 2024, 1).

66 Of the importance of compliance and its at times contradictory relationship with employee data protection, see (Eklund 2021, 81–91). As examples of studies on legal compliance, see also (Lanamäki et al. 2025; Root 2019).

1. How does EU legislation constrain and shape employers' use of ARSs that involve AI or algorithmic decision-making?
2. What legal safeguards does EU legislation provide to protect job applicants against data protection infringements and discrimination arising from the use of ARSs that involve AI or algorithmic decision-making, and how adequate are those safeguards?

These questions are examined across the four original publications and in this synthesis. Drawing on the findings, I argue that, despite the multiple constraints and conditions imposed on employers' use of ARSs, the EU-level legal framework remains inadequate to protect job applicants from the risks posed by ARSs that involve AI or algorithmic decision-making. This inadequacy stems primarily from four distinct but related factors: the vagueness of the legal parameters governing ARS deployment, the limited ex-ante oversight mechanisms, the structural barriers to enforcement by job applicants, and the inherent limitations of the available remedies.

1.3 Situating the analysis within EU law

1.3.1 EU law foundations

Before introducing the relevant areas of EU law which this dissertation bridges, the foundational characteristics of the EU legal order and its fundamental rights framework must be briefly addressed, as they shape the analytical approach adopted throughout this dissertation.

EU law constitutes an autonomous supranational legal order, distinct from both international and national legal systems, as established in *van Gend en Loos* and *Costa v ENEL*.[67] In the latter case, the Court of Justice of the European Union (CJEU) held that EU law[68] had become 'an integral part of the legal systems of the Member States and which their courts are bound to apply'.[69] Under the doctrine of direct

[67] See, e.g., C-26/62 *van Gend en Loos, p. 12* and C-6/64 *Costa v ENEL*, p. 593. See also (CJEU 1991, 6102; 2014, 32–34; Lenaerts and Gutierrez-Fons 2014, 37–38) and TEU Arts. 4–5 and 13–19.

[68] For the sake of simplicity, reference in this dissertation is made to the CJEU and EU law also in the case of pre-Lisbon Treaty case law.

[69] C-6/64 *Costa v ENEL*, p. 593.

effect,[70] EU law confers rights on individuals that are enforceable before national courts and imposes corresponding obligations on Member States and national authorities to give effect to those rights.[71] However, the scope of direct effect varies by instrument. Regulations, such as the GDPR and the AIA, are directly applicable under Article 288 of the Treaty on the Functioning of the European Union (TFEU).[72] Directives, in turn, may have only a vertical direct effect in limited situations,[73] and cannot be invoked against private parties.[74] The CJEU[75] has recognised a horizontal direct effect for certain general principles of EU law,[76] and for specific CFREU provisions,[77] which may be directly invoked in disputes between private parties, as will be discussed in more detail below in section 1.3.2.[78]

Notwithstanding direct effect, the principles of conferral and subsidiarity also preserve Member States' legislative competence in certain matters.[79] For instance, the GDPR and the AIA permit some national variation in the employment context, and the Non-Discrimination Directives allow discretion in

70 The doctrine of direct effect, originating in *Van Gend en Loos*, enables clear, precise and self-sufficient EU legal norms to produce legal effects independently of national measures, also at the individual level. See C-26/62 *van Gend en Loos*, p. 13. See also (Weilert 1991, 2413).

71 C-26/62 *van Gend en Loos*, p. 13 and (EUR-Lex 2026). See also (de Witte 2011, 326–27).

72 However, regulations' direct applicability is not absolute either, see, e.g., C-403/98 *Monte Acrosu*, paras 25–29 and (de Witte 2011, 335; EUR-Lex 2026).

73 Based on established case law, directives may have a direct effect when their unconditional and sufficiently clear and precise provisions are not adequately implemented in the Member State, see, e.g., C-41/74 *van Duyn v Home Office*, paras 13 and 15 and (de Witte 2011, 335; EUR-Lex 2026).

74 See, e.g., joined cases C-397/01 and C-403/01 *Pfeiffer and Others*, para 109. See also (Mast and Ollig 2023, 465).

75 The power to decide whether an EU act has a direct effect remains with the CJEU, see, e.g., (de Witte 2011, 332; EUR-Lex 2026).

76 The horizontal direct effect of the general principle of equal treatment on the ground of age has been acknowledged, for instance, in cases C-144/04 *Mangold,* paras 74–78 and C-555/07 *Kücükdeveci,* paras 50–51.

77 Many of the cases where horizontal direct effect has been acknowledged stem from the employment context. See, e.g., joined cases C-569/16 and C-570/16 *Bauer* and C-684/16 *Max-Planck-Gesellschaft* regarding the right to paid annual leave under CFREU Art. 31 as well as C-414/16 *Egenberger* and C-193/17 *Cresco Investigations* regarding the right to non-discrimination under CFREU Art 21. Cf. C-176/12 *Association de médiation sociale*, paras 45 and 48–49, where CFREU Art. 27 was deemed not to have a horizontal direct effect.

78 C-414/16 *Egenberger*, para 76 and joined cases C-569/16 and C-570/16 *Bauer* para 92. See also (Tridimas 2014, 390; Cecchetti 2024, 49; Mast and Ollig 2023, 468)

79 See TEU Art. 5(1)–(3).

implementation.[80] Further, procedural matters are largely governed by Member State procedural autonomy.[81] However, national discretion is ultimately constrained by the primacy doctrine,[82] established initially in *Costa v ENEL*.[83] Accordingly, where EU law conflicts with any national law, EU law prevails, and the conflicting national rule must be set aside.[84]

Tasked with ensuring the uniform interpretation of EU law across Member States, the CJEU acts as the authoritative interpreter of EU law.[85] Operating in a supranational and multilingual legal order where all the official language versions are equally authentic,[86] the CJEU adopts its own mix of interpretative methods, including textual, contextual and teleological interpretations.[87] The CJEU is particularly known for its teleological approach, whereby a provision is construed in light of the purposes of the provision itself, the legal instrument in which it is embedded, and the EU legal order as a whole.[88] This approach has enabled the CJEU to shape the substantive content of EU law beyond the text of the Treaties and secondary legislation, while also attracting criticism of judicial activism and judicial

80 While GDPR Art. 88 permits 'more specific rules' regarding employment to be enacted on the national level, AIA Art. 2(11) also explicitly allows national provisions which are 'more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers'. The Non-Discrimination Directives also allow more favourable national measures, see RED Art. 6, EED Art. 8, and GED Art. 27 and TFEU Art. 288.

81 See, e.g., C-33/76 *Rewe*, para 5 and C-45/76 *Comet*, para 13. See also (Beck 2013, 214).

82 The primacy of EU law applies as regards all EU legislation and national acts in the fields where Member States have ceded sovereignty to the EU, such as the single market (see, e.g., C-6/64 *Costa v ENEL*, p. 593-594) and in all courts of the Member States (see, e.g., C-106/77 *Simmenthal*, paras 21-22).

83 C-6/64 *Costa v ENEL*, p. 593-594. See also C-11/70 *Internationale handelsgesellschaft*, para 3. Now, there is a brief declaration (no. 17) concerning primacy also annexed to the Treaty of Lisbon, dated 13.12.2007.

84 See, e.g., C-6/64 *Costa v ENEL*, p. 594, C-11/70 *Internationale Handelsgesellschaft*, paras 2-3, C-314/08 *Krzysztof Filipiak*, paras 82-83, and C-399/11 *Melloni*, para 59. See also (de Witte 2011, 341–42; Weilert 1991, 2414).

85 See TEU Art. 19 and TFEU Art. 267. See also C-26/62 *van Gend en Loos*, p. 12, C-741/19 *Republic of Moldova*, para 45 and C-430/21 *RS*, para 52 and (CJEU 2011, 1173; 2014, 34).

86 See TEU Art. 55 and C-283/81 *CILFIT*, paras 17–18. See also (Lenaerts and Gutierrez-Fons 2014, 6–8). At the time of writing, there were 24 official language versions.

87 See, e.g., (Lenaerts and Gutierrez-Fons 2014; Beck 2013, 43; Doroga and Mercescu 2021, 94). See section 1.4.2 below for a more detailed discussion on the specifics of these methods.

88 (Hettne et al. 2011, 168; Paunio 2011, 48 and 56; Maduro 2008, 3; Lasser 2004, 229–36; Fennelly 1996, 664; Beck 2013, 289). For a more detailed discussion on teleological interpretations, see section 1.4.2 below.

law-making.[89] Nevertheless, the EU legal texts often contain deliberate vagueness that leaves interpretative leeway for the CJEU.[90]

Together, the above-discussed features of the EU legal order justify the EU-level focus adopted in this dissertation. The autonomous character of EU law means it must be approached on its own terms, rather than through the lens of any single national legal tradition.[91] Direct effect and primacy confirm that EU law directly governs individuals across the Member States,[92] establishing a baseline that national authorities must apply and respect irrespective of any additional national legislation.[93] Where EU law categorically prohibits a specific ARS use case,[94] national law adds limited value to the substantive definition of that prohibition, though it remains relevant to enforcement and remedies. Where EU law regulates ARSs, but does not categorically prohibit the relevant use case,[95] national law may impose additional substantive requirements, the permissibility of which varies depending on whether the governing instrument operates as a minimum or maximum harmonisation measure.[96] While the doctrinal framework of EU law is elaborated at the EU level, including through CJEU jurisprudence, its application to individual cases occurs primarily at the Member State level through national courts and competent authorities.[97] Accordingly, an EU-level analysis can assist stakeholders across jurisdictions in navigating relevant EU legislation and contribute to greater consistency in its application. A comprehensive mapping of national implementing legislation across all 27 Member States consequently falls outside this dissertation's scope.[98]

The EU legal order discussed above also encompasses a fundamental rights framework, which affects the analysis undertaken in this dissertation.

89 See, e.g., (Doroga and Mercescu 2021, 91). Of the criticism, see, e.g., (Neergaard and Nielsen 2011, 118–19; Maduro 2008, 5–6; Muir et al. 2013, 3; Tridimas 2013, 215–21).

90 See, e.g., (Paunio 2011, 39; Beck 2013, 57; Walkila 2015, 26).

91 While a comparative approach could have provided useful insights, such an analysis could only be reasonably conducted with considerably more limited research questions.

92 See (de Witte 2011, 358–59; CJEU 1995, 2).

93 See, e.g., Art. 4(3) TEU. The Member States have an important role in guarding the EU legal order, together with the CJEU, see also Art. 19(1) TEU and (CJEU 2011, 1168 and 1174).

94 See section 5.2.1.1 below for these types of situations.

95 Chapter 5 below offers a more detailed description of the different ways in which EU legislation may affect ARS use.

96 See the discussion regarding GDPR Art. 88, AIA Art. 2(11), RED Art. 6, EED Art. 8, GED Art. 27 and TFEU Art. 288 above. For instance, in Finland, there are numerous national provisions that affect the use of AI in recruitment, see (Publication I / Viljanen and Parviainen 2022, 2–4).

97 See TFEU Art. 19(1) and (CJEU 2011, 1168).

98 *A.C.L. Davies* has also discussed the difficulty of getting an overview of EU labour law in action in all the Member States (Davies 2012, 3–4).

1.3.2 Fundamental rights framework

Fundamental rights are at the heart of the EU's legal structure.[99] Treaty on European Union (TEU) Article 2 establishes that the EU is founded on the respect for fundamental rights, while Article 6 identifies their sources: the CFREU and the general principles of EU law.[100] Accordingly, the EU may not violate fundamental rights and must also actively take measures to ensure their wider and more effective enjoyment.[101] These requirements have direct consequences for secondary EU legislation, which must respect fundamental rights as a condition of validity[102] and be interpreted in light of them[103]. Where limitations on fundamental rights arise, CFREU Article 52(1) requires that they be provided for by law,[104] respect the essence of those rights and freedoms[105] and be proportionate[106]. When several fundamental rights clash, their protection should be reconciled, and a fair balance struck between them.[107]

99 See (CJEU 2014, 33). Fundamental rights have been protected in CJEU case law since the late 1960s. See, e.g., C-29/69 *Stauder* and C-11/70 *Internationale Handelsgesellschaft.* See also (Weilert 1991, 2417; Chalmers et al. 2024, 238–39).

100 Both the CFREU and the general principles of EU law have the European Convention on Human Rights (ECHR) and national constitutional traditions as their inspiration (see TEU Art. 6(3) and the Preamble to the CFREU). See also (Chalmers et al. 2024, 236–37).

101 (Chalmers et al. 2024, 236).

102 EU legislative acts that do not comply with fundamental rights may be declared invalid by the CJEU. See, e.g., C-236/09 *Association belge des Consommateurs Test-Achats ASBL and others.* See also (CJEU 2014, 33; Chalmers et al. 2024, 254; Lenaerts 2012, 376).

103 See, e.g., C-131/12 *Google Spain*, para 68 and cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, para 68 and (Chalmers et al. 2024, 254–58; Lenaerts 2012, 376).

104 Of this requirement, see, e.g., joined cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, paras 76–77 and joined cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert,* para 66. See also (Lenaerts 2012, 389).

105 To respect the essence of those rights, the limitations may not make the exercise of the right impossible or excessively difficult and must apply only in limited and well-defined circumstances. As examples of cases where the essence of the rights has been respected, see, e.g., C-258/14 *Florescu and Others*, paras 53–55 and C-293/12 *Digital Rights Ireland,* para 40. Cf. C-362/14 *Schrems*, para 95, where the essence of the right to effective remedies was interfered with, as the legislation did not provide any possibility for an individual to pursue legal remedies. See also (Chalmers et al. 2024, 241; Brkan 2019b).

106 To be proportionate, any limitations on fundamental rights must be necessary and either genuinely meet a general interest recognised by EU law or protect the rights of others, see CFREU Art. 52(1). See also (Chalmers et al. 2024, 241).

107 See, e.g., C-570/19 *Irish Ferries*, para 172 and C-275/06 *Promusicae,* paras 65 and 66.

The CFREU's scope of application is, however, limited. Under Article 51(1) of the CFREU, its provisions are addressed to EU institutions, bodies, offices and agencies, and it binds Member States only when they are implementing EU law.[108] Based on its wording, the CFREU does not directly address private parties such as employers and job applicants. However, four interrelated mechanisms appear to extend the effects of the fundamental rights framework to such private relationships.

First, EU secondary law may concretise fundamental rights.[109] Secondary law may, among other measures, impose obligations on private parties, the fulfilment of which contributes to the protection of fundamental rights.[110] For example, when an employer complies with the data minimisation principle under GDPR Article 5(1)(c), it thereby protects job applicants' right to data protection under CFREU Article 8, without directly invoking the fundamental right.[111] In a dispute against an employer, a job applicant may claim that the relevant provisions of secondary law are breached.

Second, fundamental rights may have a *horizontal indirect effect* affecting private relations through duties imposed on state authorities.[112] National courts as Member State organs are required to interpret EU law and the national law implementing it in conformity with fundamental rights.[113] Thus, in a dispute between private parties, the claims would be based on existing secondary law or its implementing national legislation, and the fundamental rights would operate as an interpretative constraint on the application of that law rather than as an independent basis for claims.

Third, the EU legislator has increasingly embedded fundamental rights into horizontal relations through a *horizontal meta-effect approach.*[114] When adopting the

[108] See (CJEU 2014, 33) and cases C-5/88 *Wachauf,* para 19, C-260/89 *ERT*, para 42, and C-617/10 *Åkerberg Fransson*, paras 17–21. This is a threshold that has been widely discussed in prior scholarship, see, e.g., (Lenaerts 2012, 376–87; Fontanelli 2014; Koukiadaki 2019; Publication III / Parviainen 2024, 451–55). See also section 5.2.1.2 below, where this is discussed in more detail from the point of view of CFREU Art. 21.

[109] As regards the prohibition of discrimination, see, e.g. C-441/14 *Dansk Industri*, para 23. See also (Lynskey 2015, 133; Fornasier 2015, 45; Mast and Ollig 2023, 472). However, the relationship between CFREU Art. 8 and the GDPR is less clear, see, e.g., (Lynskey 2020, 361–64).

[110] See, e.g., GDPR Art. 1 and Recital 1.

[111] Of the contested content and objectives of the right to data protection, see, e.g., (Lynskey 2020, 361–64).

[112] See, e.g., (Tridimas 2013, 214; Fornasier 2015, 32). There are different types of horizontal indirect effects, see, e.g., (Tridimas 2013, 214; Hartkamp 2013, 195–96).

[113] See, e.g., C-131/12 *Google Spain*, para 68 and cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, para 68. See also (Tridimas 2014, 390; Fornasier 2015, 32; Mast and Ollig 2023, 466).

[114] This term is proposed by *Mika Viljanen* (Viljanen 2024, 3–4). Other scholars have also discussed this phenomenon, but with varying terminology, and particularly from the point of view of platform law, see (Mast and Ollig 2023).

horizontal meta-effect approach, the legislator assigns the task of concretising fundamental rights to private parties.[115] In this approach, organisations are not directly forced to comply with, implement or enforce the fundamental rights as such.[116] Rather, the legislation requires them to (i) set up processes to identify, analyse and evaluate certain fundamental right risks and impacts of their action, (ii) plan responses to these risks and impacts, and (iii) implement and act on the plans.[117] Both the GDPR and the AIA employ this strategy, making fundamental rights a topic of organisational concern.[118] The rationale is apparently that acknowledging fundamental rights in internal processes leads to greater respect for those rights and fewer violations.[119] However, the internal processes required might become mere tick-the-box exercises, with fundamental rights considerations treated as one standard among others.[120] To make matters worse, job applicants struggle to challenge such internal processes, as will be discussed in sections 6.1.1.4 and 6.2 below.[121]

Fourth, the CJEU has recognised a *horizontal direct effect*[122] for certain fundamental rights enshrined in the CFREU, including the right to non-discrimination[123] and the right to an effective remedy[124]. Based on CJEU case law, a CFREU provision can have a horizontal direct effect where it is 'sufficient in itself'

115 *Tobias Mast* and *Christian Ollig* have thus accused the EU legislator 'of being somewhat lazy', (Mast and Ollig 2023, 486).

116 (Viljanen 2024, 4 and 12).

117 (Viljanen 2024, 4 and 12). As Viljanen notes, for instance, AIA Art. 9(2) requires the identification and analysis of the known and reasonably foreseeable risks that high-risk AI systems may pose to fundamental rights, and the adoption of appropriate and targeted risk management measures designed to address these risks. However, in AIA Art. 9(5) the requirement is lowered to require only measures that make the relevant residual risk such which is 'judged to be acceptable'.

118 See, e.g., (Viljanen 2024). See, e.g. GDPR Art. 35 and AIA Arts. 9, 26(5) and 27. Deployers of high-risk AI systems are also required to monitor whether the system presents a risk to fundamental rights, as meant by AIA Art. 79(1).

119 (Viljanen 2024, 4 and 14–15).

120 (Viljanen 2024, 8–11; Mast and Ollig 2023, 479–80).

121 See also (Viljanen 2024, 15). Of the job applicants' lacking remedies under the AIA, see also (Publication IV / Parviainen 2026).

122 Horizontal direct effect is not a unitary phenomenon, see, e.g., (Cecchetti 2024, 48–49; Fornasier 2015). A broader reading of horizontal direct effects includes situations where the dispute involves two private parties and one of them refers to the incompatibility of national measures with EU law to trigger the disapplication of a national measure, which indirectly impacts the private relationship (see, e.g., C-144/04 *Mangold* and C-555/07 *Kücükdeveci*). Whereas, a stricter reading includes only situations where absent EU or Member State law or other public measures, a private party is directly bound by the fundamental rights (see, e.g., joined cases C-659/16 and C-570/16 *Bauer*, para 85).

123 See, e.g., C-414/16 *Egenberger*, para 76 and C-193/17 *Cresco*, paras 76 and 85.

124 See, e.g., C-414/16 *Egenberger*, para 78.

to confer a right on individuals without requiring further legislative specification, and the situation falls within the scope of EU law.[125] Where a horizontal direct effect for a fundamental right is accepted, a private party may directly rely on that right against another party as long as the situation falls within the scope of EU law.[126] I have argued in Publication III that job applicants could directly invoke CFREU Article 21, for instance, where an automated decision has discriminated against them on the grounds of a characteristic that is protected under CFREU Article 21 but not under the Non-Discrimination Directives.[127] Job applicants might also invoke the right to an effective remedy in the opaque algorithmic recruitment context, particularly if procedural rules are insufficient to enable them to pursue EU-law-based claims in practice.[128]

While several fundamental rights may be affected by algorithmic recruitment, three fundamental rights are particularly central in this dissertation: the right to protection of personal data (CFREU Article 8), the right to non-discrimination (CFREU Article 21), and the right to an effective remedy (CFREU Article 47), which supports the exercise of the other fundamental rights.[129] First, the EU secondary law instruments to be examined are selected because they assist in safeguarding the rights to the protection of personal data and non-discrimination.[130] Second, these fundamental rights guide the interpretation of secondary law instruments, along with other relevant rights such as employers' freedom to conduct a business (CFREU

125 See, e.g. cases C-414/16 *Egenberger*, paras 76 and 78 and joined cases C-659/16 and C-570/16 *Bauer*, para 85. Cf. C-176/12 *Association de médiation sociale*, paras 44-51, and C-196/23 *Plamaro*, paras 49–55. See also (Frantziou 2019, 318–19; Mast and Ollig 2023, 468).

126 See C-414/16 *Egenberger*, para 76 and joined cases C-659/16 and C-570/16 *Bauer*, para 92. See also (Tridimas 2014, 390; Mast and Ollig 2023, 468; Cecchetti 2024, 49).

127 (Publication III / Parviainen 2024, 451–55). However, the scope of application of the CFREU complicates the additional protection provided by the CFREU Art. 21, see also CFREU Art. 51 and TEU Art. 6(1). See also section 5.2.1.2 below.

128 See (Publication IV / Parviainen 2026) and section 6.3 below.

129 Of the risks ARSs may pose on these rights, see section 1.1.1 above. For instance, the right to privacy (CFREU Art. 7) could also be affected. Moreover, closely related to CFREU Art. 21 are the rights to equality before the law (CFREU Art. 20) and equality between women and men (CFREU Art. 23). Furthermore, the right to human dignity (CFREU Art. 1), freedom to choose an occupation and right to engage in work (CFREU Art. 15) and integration of persons with disabilities (CFREU Art. 26) could also be impacted. However, to keep the scope manageable, I do not examine these rights in detail.

130 See section 1.4.3 below for a more precise description of the scope of the framework.

Article 16)[131] and right to property (CFREU Article 17).[132] Third, the potential horizontal direct effect of the rights to non-discrimination and to an effective remedy is also acknowledged in the analysis.

With the relevant EU law and fundamental rights framework introduced, the following section turns to this dissertation's positioning and limitations.

1.3.3 Positioning and limitations

Since ARSs do not neatly align with any single field of law,[133] this dissertation bridges several areas of EU law.

EU labour law constitutes the first of this dissertation's disciplinary anchor points, given that recruitment is the core subject herein. EU labour law comprises mainly directives governing Member States' regulation of labour markets,[134] covering areas such as freedom of movement, equality, health and safety, working conditions, rights on restructuring and collective labour law.[135] However, as noted in section 1.1.1, most EU labour legislation does not apply to job applicants, who are not yet in an employment relationship and therefore not in a position of subordination

131 See, e.g. C-426/11 *Alemo-Herron,* where the essence of the freedom to conduct a business was deemed to be adversely affected, when the transferee was unable to participate in collective bargaining and it seriously reduced its contractual freedom (paras 31–37). See also C-70/10 *Scarlet Extended*, paras 45–49, where the freedom to conduct a business was noted as a constraint on obligations imposed on private parties deploying automated systems.

132 Of the balancing, see section 1.4.2 below. Some secondary law provisions also require balancing of the employers' and job applicants' rights and interests, see, e.g., GDPR Art. 6(1)(f).

133 See also (Abraha 2023, 172; Baldini and De Benedetto 2025, 1645). However, EU law appears to be less inclined than national legal systems to compartmentalise laws into distinct fields, see, e.g., (Tuori 2011, 161; van Gestel and Micklitz 2011, 57).

134 (Davies 2012, 3–4). See also TFEU Articles 152 and 154–155, which facilitate social dialogue between EU-level trade unions and employers' associations that could reach agreements. The social partners at the EU level have reached an autonomous Framework Agreement on Digitalisation (FAD) that also covers the use of AI in the workplace, including in recruitment. The FAD establishes a model partnership process between employers and workers' representatives to be applied when deploying digital technologies in the workplace. Substantively, the FAD lists only certain approaches and measures that employers, workers, and their representatives can utilise when AI systems are deployed. Since the FAD does not create directly binding legal parameters in Member States, its provisions will not be studied in detail in this dissertation. However, to the extent that the FAD is implemented on the national level, collective agreements may create binding legal constraints on AI use in certain Member States and sectors.

135 See, e.g., (Barnard 2012) and TFEU Art. 153.

or dependency with respect to a specific employer.[136] The Non-Discrimination Directives are a significant exception:[137] they also apply during the recruitment process and aim to combat discrimination and put into effect the principle of equal treatment therein.[138]

Non-discrimination could alternatively be approached within the independent discipline of EU anti-discrimination law,[139] rather than as part of EU labour law.[140] While scholarship on EU anti-discrimination law has been an important source, particularly in Publication III, this dissertation is positioned rather in EU labour law for the following reasons. First, non-discrimination in the employment context has traditionally been taught and researched within EU labour law, where it plays an important role.[141] Second, algorithmic discrimination does not pose an exception to this tradition: labour law journals have published some of the prior studies on algorithmic discrimination in the employment context.[142] Third, this dissertation focuses specifically on the use of AI and other algorithmic systems by employers rather than commercial deployers more broadly. However, EU labour law, on its own, is insufficient to address all the dimensions of algorithmic recruitment.[143]

Accordingly, *EU data protection law* is the second disciplinary anchor of this dissertation.[144] Given the EU labour law's limited reach during the recruitment phase, the GDPR plays a significant supplementary role. It is 'binding in its entirety

136 See, e.g., (Davidov 2017, 374; Weiss 2011, 48; Davidov 2016b, 119; Hendrickx 2018, 200; Gramano 2024). As the applicants are not obliged to follow employers' orders or to continue the recruitment process, no similar subordination to the employer exists, as with employees. Of subordination in the recruitment phase, see also (Lacková 2022, 73–74).

137 Regulation on freedom of movement for workers within the union (EU) 492/2011 is also applicable in the recruitment context, prohibiting nationality-based discrimination. However, it concerns the free movement dimension of access to employment rather than the governance of AI or algorithmic decision-making. Accordingly, for the purposes of this dissertation, the regulation's provisions offer limited analytical purchase beyond what is already addressed through the Non-Discrimination Directives and the CFREU.

138 Of the aims of the Non-Discrimination Directives, see RED Art. 1, EED Art. 1 and GED Art.1, and of the scope of application, see RED Art. 3, EED Art. 3, GED Art. 14.

139 The non-discrimination questions could also be viewed as part of the more general EU fundamental rights law, see, e.g., (Muir 2018).

140 (Belavusau and Henrard 2019, 616).

141 See, e.g., (Davies 2012, 109–72; Barnard 2012, 256–498).

142 See, e.g., (Parodi 2024; Kelly-Lyth 2023; Abraha 2023). However, the discussion of algorithmic discrimination in recruitment has also appeared in more general (Kelly-Lyth 2021; Carter 2024; Grozdanovski 2021) or technical law journals (Rigotti and Fosch-Villaronga 2024).

143 See section 1.1.1 above.

144 Of the foundations of EU data protection law, see, e.g., (Lynskey 2015; Kuner et al. 2020; Bygrave 2002).

and directly applicable' in all Member States[145] and applies fully during recruitment whenever personal data is processed.[146] Since the evaluation of job applicants' suitability necessarily involves the processing of personal data, the GDPR applies to most phases of algorithmic recruitment.[147] Data protection law can therefore address, for instance, certain informational gaps that EU labour law leaves open.

However, protecting individuals is not the only objective of the GDPR. The GDPR pursues a dual purpose.[148] Under Article 1(2), it 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'[149], while Article 1(3) states that it aims to ensure the free flow of personal data within the EU, which data protection should not restrict or prohibit.[150] When applying the GDPR, these two purposes must be balanced.[151] Despite its aim to protect fundamental rights beyond the right to the protection of personal data,[152] the GDPR does not address all the risks posed by AI systems.[153]

145 TFEU Art. 288.

146 In algorithmic recruitment, the processing is conducted by automated means in a professional capacity, making the GDPR applicable if personal data is processed (GDPR Art. 2). Nevertheless, there may arise some problematic questions regarding the territorial scope of the GDPR, if the employer utilising algorithmic recruitment is not established in the EU. In some situations, the ARS may monitor the behaviour of the job applicants in the EU, putting the processing in the scope of the GDPR (GDPR Art. 3(2)(b), see also (EDPB 2019b, 19–20)). However, if there is no monitoring, it should be analysed whether the recruitment process that may lead to a job offer is targeted to EU job applicants and whether it counts as offering a service (GDPR Art. 3(2)(a)). The EDPB has considered that human resource management does not count as an offer of service (EDPB 2019b, 18). Thus, the algorithmic recruitment process of an employer not established in the EU might not fall within the scope of GDPR Art. 3(2)(a).

147 However, there might also be ARSs that do not process personal data, such as systems that draft job advertisements, which would fall out of the GDPR's scope.

148 Of the dual objectives of EU data protection regulation, see also (Hijmans 2020, 56–58; Lynskey 2015, 46–88).

149 See also CFREU Art. 8(1) and TFEU Art. 16(1) and GDPR Recitals 1 and 2, which emphasise the fundamental rights basis of the regulation. See also GDPR Recital 10.

150 GDPR Recital 2. See also GDPR Recitals 7 and 10.

151 For instance, *Hielke Hijmans* has concluded that after the Lisbon Treaty entered into force, the protection of fundamental rights has been more prominent, although the free movement of data is still sometimes mentioned by the CJEU (Hijmans 2020, 53).

152 See GDPR Recital 4 listing the fundamental rights which the GDPR particularly observes: 'the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity'. See also (Hijmans 2020, 50–51 and 57).

153 For instance, the decisions that are based on algorithmic decision-making but not fully automated are not subject to specific protections under the GDPR, cf. AIA Art. 86 and 26(11).

Thus, the *EU AI regulation* occupies a distinct but complementary role. For instance, the AIA's provisions on personal data processing[154] intersect with the GDPR,[155] its information disclosure obligations[156] supplement EU labour law's rights to information and consultation,[157] and its implications for non-discrimination and effective remedies touch on fundamental rights law[158]. Many of the AIA's rules appear to be designed also to protect the affected persons and their fundamental rights.[159] However, compared to the Non-Discrimination Directives and the GDPR, the AIA has more internal market-enhancing objectives.[160] According to AIA Article 1(1) it aims 'to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation'.[161] The AIA's treaty basis[162] and the more risk-based,[163] product-safety approach also appear to emphasise the market-integration aims.[164] Nevertheless, identifying the AIA's primary objective appears challenging.[165] That is problematic, since the objectives of the EU legal instruments bear on their teleological interpretation, as discussed in section 1.4.2.

Since this dissertation's substantive scope is limited to the *use* of AI and other algorithmic recruitment systems,[166] the legal constraints governing the development

154 See, e.g., AIA Arts. 10(5) and 26(4).
155 See also AIA Art. 2(7) and Recital 10.
156 See AIA Arts. 26(7) and 26(11).
157 See, e.g., CFREU Art. 27, the Information and Consultation Directive and (Brameshuber 2021). However, as mentioned in section 1.1.1, the rights to information and consultation do not appear to protect job applicants.
158 The term EU fundamental rights law appears in prior scholarship, see, e.g. (Tuori 2017; Chalmers et al. 2024). Cf. (Douglas-Scott and Hatzis 2017) on EU law and human rights.
159 (van Eecke and Regenhard 2024, 9–10). See, e.g., AIA Art. 5 and AIA Chapter III, Section 2.
160 See also (van Eecke and Regenhard 2024, 8).
161 See also AIA Recitals 6–8.
162 The legal basis of the AIA is mainly in TFEU Art. 114 (and TFEU Art. 16 only to the extent that there are specific rules on processing of personal data in the law enforcement context) and the GDPR is based on TFEU Art. 16.
163 See AIA Recital 26.
164 See e.g., (Leufer and Hidvegi 2023, 164–67; van Eecke and Regenhard 2024, 8–9).
165 See, e.g., (van Eecke and Regenhard 2024, 10).
166 The use phase is the most directly relevant to employers and job applicants and also critical for fundamental rights protection. See AIA Recital 93 and (Demkova 2024; European Union Agency for Fundamental Rights 2020).

phase fall largely outside the scope of the analysis.[167] From the perspective of the AIA, this means that the providers' obligations, which form the core of the AIA's substantive requirements, are excluded from the scope.[168] The focus is also limited to systems specifically developed for the recruitment context.[169] Thus, the distinct legal questions raised by the use of general-purpose AI systems as such fall outside the scope of this dissertation.[170] Furthermore, agentic AI systems fall largely outside this dissertation's scope. While section 3.3.3 briefly introduces the concept to contextualise emerging developments in AI deployment, a substantive legal analysis of agentic AI in the recruitment context remains beyond the scope of the analysis conducted here, partly reflecting the stage of their development at the time of writing most of the original publications.[171]

Despite the relevance of fundamental rights, I do not position this dissertation as a study of fundamental rights law. First, the main focus herein is on the concrete safeguards[172] EU secondary legislation provides, in particular, obligations relating to data protection and non-discrimination that either directly or through national implementation measures bind private employers. Second, I focus on the EU level and do not analyse in detail the European Convention on Human Rights (ECHR)[173]

167 The development of AI and algorithmic decision-making systems raises distinct legal questions, including issues related to data protection, copyright and potentially compliance with the requirements set for general-purpose AI systems in the AIA (see (Hacker 2021; Publication I / Viljanen and Parviainen 2022; Hacker et al. 2023; Gstrein et al. 2024). However, decisions made during development, such as whether personal data is retained in the model, can influence the legality of deployment and the employers' obligations. See (EDPB 2024b, 4) and section 5.2 below.

168 See (Cristofolini 2024, 86) where it has been considered that analysis of AI's impact on workers should also cover the provider and their obligations under the AIA. In Publication I, developers' obligations were also noted, but the AIA was then only at the initial proposal stage and not covered in detail. On the AI development phase in prior research, see, e.g. (Hacker 2021; Kramcsák 2023).

169 As will be discussed below in section 3.3.2, LLM-based recruitment systems developed through fine-tuning and tailoring them specifically for recruitment needs are, nevertheless, central in this dissertation.

170 As will be explained in section 2.5 below, the employer might then be considered a provider of a high-risk AI system, and the providers' obligations arising in such situations are not covered here.

171 When utilising agentic AI in the high-risk recruitment use cases, employers may often be deemed as providers under the AIA. See AIA Art. 25(1) and section 2.5 below.

172 In *Luigi Ferrajoli*'s distinction between fundamental rights and their safeguards, the focus in this dissertation is on the latter. See (Ferrajoli 2001, 23–29).

173 Convention for the Protection of Human Rights and Fundamental Freedoms, 4.11.1950.

or other international conventions.[174] Hence, as regards fundamental rights, the examination focuses on the CFREU, which, unlike many of its international counterparts, contains certain provisions directly enforceable against private actors[175] and a specific right to the protection of personal data[176]. Similarly to the CJEU, I do not often cite the ECHR directly.[177] Still, I acknowledge that the ECHR provides the foundation for many rights in the CFREU[178] and interpretations of the CFREU must be aligned with those of the ECHR where rights correspond.[179]

Furthermore, there are a few additional limitations. Importantly, the analysis is restricted to job applicants pursuing private employment relationships with traditional employers. As a result, several noteworthy issues, such as the protection of persons seeking platform work[180] and public service-related questions,[181] are excluded. Finally, the temporal scope of this dissertation extends to the end of October 2025.[182]

Taken together, this dissertation is best characterised as an EU labour law and data protection study that engages with AI regulation and fundamental rights across its analysis.

174 Thus, the United Nations (UN), Council of Europe (COE) and International Labour Organization (ILO) conventions are also excluded from the scope of this dissertation. However, these conventions, such as the Convention 108 of the COE, have also affected the relevant EU legislation.

175 See section 1.3.2 above.

176 CFREU Art. 8. However, the COE's Convention 108 for the protection of individuals with regard to the processing of personal data (and its modernised version 108+) is specifically about data protection, and the CFREU Art. 8 draws from the Convention.

177 Of the CJEU's tendency not to explicitly cite the ECHR or ECtHR case law, see (de Búrca 2013, 174–75).

178 See preamble of the CFREU and Explanations to the specific provisions. According to the Explanations, CFREU Art. 8 on the protection of personal data is partly based on ECHR Art. 8, CFREU Art. 21 draws on ECHR Art. 14, and CFREU Art. 47 is based on ECHR Art. 13.

179 CFREU Art. 52(3). According to the Explanations to the CFREU (p. 17–19), the meaning and scope of the CFREU Arts. 8, 20, 21 and 23 do not appear to fully correspond with those of the ECHR. However, the parts of the CFREU Art. 47 that refer to a fair trial correspond mostly to those of ECHR Art. 6(1). Yet, as noted in CFREU Art. 52(3), the CFREU may also provide more extensive protection than the ECHR.

180 Regarding recruitment in platform work in general, see, e.g., (Williams et al. 2021).

181 On the use of AI in public sector recruitment, see, e.g. (Keppeler 2024).

182 Consequently, for instance, the Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) and Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) have not been considered in detail when writing this dissertation.

1.4 Methodology

1.4.1 Methodological approach

Achieving the objectives introduced in section 1.2 requires generating new knowledge about the content of valid EU-level legislation governing algorithmic recruitment across multiple fields of law.[183] To that end, this article-based dissertation employs primarily a problem-based legal dogmatic approach with a systematising component. The remainder of this section outlines the approach, while sections 1.4.2 and 1.4.3 explain how interpretation and systematisation are conducted in practice in this dissertation.

As noted by *Aulis Aarnio,* legal dogmatic studies aim to produce the most reliable possible account of the content of the legal system.[184] Two established tasks characterise legal dogmatics in their effort to realise this objective: the interpretation and systematisation of (valid) legal norms.[185] Yet, legal dogmatic studies can be conducted in various ways.[186]

Problem-based legal dogmatics address a specific problem[187] by examining all norms across the legal system[188] that affect or aim to resolve it.[189] Problem-based legal dogmatics is particularly useful when multiple legal frameworks are used to

183 See also section 1.1.1 and 1.3.3 above.

184 (Aarnio 2011, 12).

185 See, e.g., (Peczenik 1983, 118; Aarnio 2011, 1; 1978, 52). For instance, *Raimo Siltala* also includes weighing and balancing legal principles and other legal standards as a distinguishing feature of legal dogmatics (Siltala 2003, 328).

186 See, e.g., (Siltala 2003, 507–92).

187 *Kaius Ervasti* has explained that in problem-based legal dogmatics, the research problem is formed based on questions that arise in practice rather than centring on some clear juridical matter. Thus, according to Ervasti, selecting a research object and formulating the research problem requires empirical knowledge. See (Ervasti 2000, 581). The research problem for this dissertation emerged in 2019, inspired by court training, work experience as an employment lawyer, and studies in business law and human resources. I observed the increasing offering of algorithmic systems in recruitment and workforce management, which raised multiple legal questions that I began exploring in my Master's thesis in 2020 (Parviainen 2020).

188 (Kangas 1982, 385–86; 1997, 94; Aarnio 2011, 12). Cf. In traditional legal dogmatics, the fields of law may restrict how legal problems are identified and defined (Tuori 2011, 161), shape the types of questions that can be asked and limit the range of possible answers (Aarnio 1978, 93). *Urpo Kangas* noted in his dissertation that traditional legal dogmatic research alone is insufficient for forming a comprehensive overview (Kangas 1982, 384).

189 (Kangas 1997, 93). Cf. Of a broader 'problem- and interest-oriented approach' see (Bygrave 2002, 10).

solve the problem at hand,[190] such as in the case of addressing the data protection and non-discrimination risks arising from employers' use of ARSs. Yet, labelling a study as problem-based legal dogmatics mostly reflects how the research problem is addressed, but tells little about how the study is actually conducted. In this dissertation, practical legal dogmatics has been significant, although the dissertation also comprises a systematising part.

Practical legal dogmatics focuses on the interpretative task,[191] aiming to clarify the normative content of the legal norms.[192] The legal texts are often ambiguous or vague, and carry various meanings.[193] Practical legal dogmatics aim to interpret the legal text to assign[194] or find a meaning to those and provide interpretative recommendations.[195] These interpretative recommendations may guide legal practitioners, including judges, in construing legal norms.[196] Since legal scholars may utilise various methods of interpretation and end up proposing varying interpretations, argumentation that justifies the proposed interpretation is crucial.[197]

The doctrine of the sources of law determines which materials can legitimately support legal argumentation. Considering the CJEU's central role as the authoritative interpreter of EU law,[198] I use the same sources and methods of interpretation as the CJEU.[199] Adhering to the same sources and methods as the CJEU does not preclude critiquing[200] its interpretations or proposing alternatives,[201] since interpretative

190 (Smits 2017, 226–27).

191 Interpreting texts has always been part of legal scholars' tasks, see (van Hoecke 2013, 4).

192 (Aarnio 2011, 13 and 104–5; 1989, 288).

193 (Aarnio 2011, 47; 1978, 70–71). In EU legislation, these are common features due to the numerous official language versions and the political compromises that may result in deliberately ambiguous wordings, see, e.g., (Paunio 2011, 39; van Gestel and Micklitz 2011, 67; Walkila 2015, 26).

194 (Makkonen 1981, 132; Rautiainen et al. 2023, 161–62; Paunio 2011, 39).

195 (Aarnio 2011, 30; 1982, 61). Assigning refers to construing a norm based on legal sources, whereas finding implies that the norms already exist and the interpreter simply identifies them in the legal sources. See, e.g., (Rautiainen et al. 2023, 162)

196 (Bengoetxea 1993, 226; Aarnio 2011, 44–45). Hence, while studying the legal order, legal dogmatics also 'contributes to the production and reproduction of the legal order, and participates in ongoing legal discourse', which *Kaarlo Tuori* has termed as 'the dual citizenship' of legal dogmatics (Tuori 2011, 6–7). In the context of EU law, see also (Gadbled and Muir 2022, 626).

197 (Aarnio 2011, 39; van Hoecke 2013, 5).

198 See section 1.3.1 above.

199 See sections 1.4.2 and 1.5 below.

200 See (Aarnio 2011, 44). As an example of critical reading of the legal reasoning of the CJEU, see, e.g., (Conway 2012, 52–84). Cf. Of the risk of 'case law journalism' see, e.g. (van Gestel and Micklitz 2014, 299; Schlag 2007).

201 See also (Beck 2013, 29).

latitude remains.[202] At the same time, working with the sources and methods accepted by the CJEU should lead to interpretation suggestions that remain viable in judicial practice.[203]

The practical legal dogmatics is interconnected with its theoretical counterpart.[204] Namely, the systematisation task characteristic of theoretical legal dogmatics[205] presupposes an understanding of the content of legal norms that practical legal dogmatics supplies.[206] Conversely, systematisation can influence the interpretation of legal norms and reveal systematic connections that are not apparent from reading individual provisions in isolation.[207]

Systematisation generally encompasses the construction of concepts, principles, doctrines, and theories.[208] Though the techniques used vary depending on the topic, tradition, and purpose of the systematisation.[209] The purpose may be, for instance, to organise positive legal norms into a coherent, internally consistent structure that can guide interpretation of the law, enhance the predictability of legal decision-making,[210] and assist in navigating complex, fragmented and dispersed legislation.[211] Since EU legislation governing ARSs is relatively complex and scattered across multiple fields of law, systematisation is warranted here. The output of the systematisation is presented mainly in this synthesis, but it builds upon the Publications I-IV.[212]

Three main factors drove the decision to adopt an article-based format for this dissertation.[213] First, the format accommodates the dynamic regulatory and technological landscape by allowing each publication to respond to the developments at the time of writing. Second, it facilitates external peer review and

202 See section 1.4.2 below.
203 See also (Beck 2013, 17–20).
204 (Aarnio 1978, 93; Rautiainen et al. 2023, 135, 217).
205 (Aarnio 2011, 104; 1989, 302; Rautiainen et al. 2023, 135).
206 See also (Aarnio 1978, 93; Rautiainen et al. 2023, 135, 217).
207 See also (Aarnio 1978, 93; 1989, 293; Rautiainen et al. 2023, 135, 217).
208 See, e.g., (Aarnio 1978, 52; Tuori 2011, 173). A traditional example of systematisation is a legal taxonomy, see, e.g., (Aarnio 1978, 74). The classification of law into distinct fields is also a product of legal systematisation (Koivisto 2015, 955).
209 (Smits 2017, 217 and 224). However, as *Pauli Rautiainen et al.* have pointed out, there are relatively few accounts on how the systematisations are made in practice (Rautiainen et al. 2023, 207).
210 (Smits 2017, 211–12 and 216).
211 (Smits 2017, 216; Aarnio 2011, 97–98; 1978, 74). *Ida Koivisto* has aptly described systematisation as the arrangement of parts of the law in such a way that the resulting whole becomes more illustrative, coherent and comprehensible than those parts of law are in their original context (Koivisto 2015, 955).
212 See Chapters 2, 5 and 6.
213 Of article-based dissertations in Finnish legal scholarship, see, e.g., (Halila 2015, 1122).

scholarly feedback during the research process.[214] Third, the format enables thematic and methodological variation across publications. However, the format also imposes constraints, as journal article length requirements necessitate narrow, specific research questions and selective choices regarding scope.

While legal dogmatic analysis of the law as it is (*de lege lata*) provided a consistent methodological anchor across all publications, the article-based format also permitted supplementary approaches, which particularly Publications I and IV utilised. Publication I combined legal dogmatic analysis with two fictional case studies[215] under Finnish law[216] and a grounded theory approach[217] to develop a heuristic stratigraphy of AI law.[218] Instead, Publication IV extends beyond de lege lata analysis to offer suggestions as to what the law should be (*de lege frenda*)[219], examining potential enhancements to the remedies available to job applicants, including through legislative reform.[220] These suggestions arise from the legal-dogmatic analysis itself,[221] specifically from the identification of shortcomings in the current text of the AIA, rather than from a systematic normative inquiry designed primarily to assess and propose legislative change.[222] Comprehensive policy recommendations remain outside the scope of this dissertation. Accordingly, apart from Publication IV, the solutions proposed here are mostly interpretative

214 Especially in Publication III, the anonymous peer reviewer feedback affected the approach ultimately chosen.

215 The two fictional cases, private sector recruitment and public sector COVID-19 contact tracing app, were chosen from domains where AI legislation was presumably rich and important (Publication I / Viljanen and Parviainen 2022, 2).

216 The EU law's significant influence on national legislation in this area, as discussed above in section 1.3, explain this approach, although national deviations also exist.

217 *Barney Glaser* and *Anselm Strauss* define grounded theory as a theory discovered from data. According to them, grounded theories could be better suited to their supposed uses than theories 'generated by logical deduction from a priori assumptions' (Glaser and Strauss 1968, 1, 3, 6).

218 (Publication I / Viljanen and Parviainen 2022, 2).

219 For instance, *Raimo Siltala* has referred to this type of research as de lege ferenda studies on law or as research of legal politics (Siltala 2003, 933). Such studies typically aim to assist the legislator in producing alternative regulatory solutions. Of the different types of de lege ferenda studies on law, see, e.g., (Leskinen 2022; Siltala 2003, 126, 131–32; Linna 1987, 21–22).

220 (Publication IV / Parviainen 2026). In addition to legislative changes, I also propose additional guidance by the authorities, standards, and informational campaigns. Bygrave has noted the difficulties in drawing the line between de lege lata and de lege ferenda in data protection law, see (Bygrave 2002, 15–16).

221 Of de lege ferenda suggestions as byproducts of the legal dogmatic analysis, see also (Määttä 2016, 108).

222 A Finnish example of a comprehensive de lege ferenda study is *Tuula Linna*'s dissertation (Linna 1987). For a more recent account of the de lege ferenda research as a method and discipline, see, e.g., (Leskinen 2022).

suggestions regarding current valid and binding EU legislation, or practical suggestions for employers' compliance or job applicants' enforcement efforts. The interpretative methods underlying these contributions are outlined in the following section.

1.4.2 Interpretation

Identifying and interpreting all valid EU-level legal norms that constrain or shape employers' use of ARSs and that protect job applicants against data protection infringements and discrimination constitutes this dissertation's foundation.[223] However, before the legal analysis can proceed, and in parallel with it, engagement with technical and non-legal scholarship is also necessary to establish a factual and technical understanding of how ARSs operate, what risks they pose, and how ARSs have evolved.[224]

The EU legislation examined in this dissertation is often vague or ambiguous,[225] at times technically complex,[226] and spread across multiple legislative instruments.[227] These features complicate the interpretative task and necessitate recourse to the combination of interpretative methods[228] and sources that the CJEU employs[229]. This dissertation utilises the three classical methods, namely *textual*, *contextual* and

223 (Nielsen 2013, 77). Of this kind of a mapping stage in doctrinal legal research, see (Hutchinson and Duncan 2012, 110).

224 See section 1.5 below.

225 See, e.g., GDPR Art. 22(1) provision on 'a decision based solely on automated processing' and Art. 15(1)(h) on 'meaningful information about the logic involved' and AIA Art. 86(1) on 'clear and meaningful explanations of the role of the AI system […] and the main elements of the decision taken'.

226 See, e.g. AIA Art. 10 on data and data governance, Art. 11 on technical documentation and Art. 13 on transparency and provision of information to deployers.

227 These are common elements in EU law, see, e.g., (Beck 2013, 172–73).

228 According to settled case-law of the CJEU, when 'interpreting a provision of EU law, it is necessary to consider not only its wording, but also the context in which it occurs, and the objectives pursued by the rules of which it is part'. See, e.g., cases C-203/22 *Dun & Bradstreet*, para 39, C-487/21 *Österreichische Datenschutzbehörde and CRIF*, para 19, and C-597/21 *Pankki S*, para 38. These methods were already noted in the C-26/62 van Gend en Loos (p. 12), but in reverse order.

229 The sources CJEU considers include EU primary and secondary law, CJEU case law, general principles of EU law, international law, common constitutional traditions of Member States, EU soft law, and preparatory works, see, e.g., (Bengoetxea 1993, 225–27; Komárek 2015, 44). Judges may also consider sources not often explicitly cited in the judgements, such as EU authorities' guidance and academic writings. See, e.g., (Komárek 2015, 44–45; Siltala 2003, 474–75; Hettne et al. 2011, 120–22). Of the direct use of Article 29 Working Party (WP29) guidance, see, e.g., case C-203/22 *Dun & Bradstreet Austria*, para 45.

teleological interpretations,[230] in construing the provisions governing ARSs and draws on the sources as interpretative aids where relevant.[231] The classical methods of interpretation are used with differing weights depending on the characteristics of the provision under examination.[232] Although discussed separately below, in practice, these methods are closely intertwined.[233]

Textual interpretation[234]*,* which deduces the meaning of the legal norm from its literal expression, i.e. wording and syntax, is the point of departure.[235] In EU law, textual interpretation in its purest form[236] would require examination of all the authoritative language versions.[237] As a rule, where the wording is clear and precise, contextual or teleological interpretations should not override the literal meaning for the sake of legal certainty.[238] However, given the multilingualism, deliberate vagueness, abstract drafting style, and value pluralism of EU legislation, textual

230 These three methods have been broadly discussed in prior scholarship, see, e.g., (Lenaerts and Gutierrez-Fons 2014; Beck 2013, 293), although sometimes with different terminology, cf. e.g., (Maduro 2008, 3; Paunio 2011, 45; Schermers and Waelbroeck 2001, 10). However, the list is not exhaustive as the CJEU also uses other methods of interpretation, such as a comparative law method (Lenaerts and Gutierrez-Fons 2014, 44–52; Hettne et al. 2011, 159–63) and consistent interpretation in light of international and Member State law (Lenaerts and Gutierrez-Fons 2014, 37–51, 61).

231 See section 1.5 below for a more detailed discussion on the sources.

232 Among other factors, the ambiguity and the context of the provision affect the weight and importance of each method. Similarly, in the CJEU case law, the relative weight of the different interpretation methods appears to vary (Beck 2013, 293 and 298–300).

233 See also (Lenaerts and Gutierrez-Fons 2014, 61). In this dissertation, contextual and teleological interpretations are often interrelated, and, for instance, recitals simultaneously inform both.

234 At times this is also referred to as linguistic, grammatical, semiotic, or literal interpretation, see, e.g., (Paunio 2011, 45–48; Komárek 2015, 45).

235 Of textual interpretation in prior research, see, e.g., (Lenaerts and Gutierrez-Fons 2014, 8; Beck 2013, 188; Neergaard and Nielsen 2011, 99; Hesselink 2011, 200–201; Schermers and Waelbroeck 2001, 10–11; Komárek 2015, 45–46).

236 *Elina Paunio* has pointed out that the CJEU, however, does not appear to compare the different language versions systematically (Paunio 2011, 45). For a recent example of such a limited comparison, see, e.g., C-203/22 *Dun & Bradstreet Austria*, paras 40–41.

237 See, e.g., cases C-283/81 *CILFIT v Ministero della Sanitá*, paras 18–19 and C-476/11 *HK Danmark*, para 42 and (Schermers and Waelbroeck 2001, 11–13; Komárek 2015, 45; Lenaerts and Gutierrez-Fons 2014, 59). For an individual scholar, language proficiency sets the practical limits of textual interpretation, rendering the multilingual approach of *CILFIT* (C-238/81) practically unattainable, despite the surface-level assistance AI translation tools may provide.

238 See, e.g. case C-220/03 *ECB v Germany*, para 31. See also (Lenaerts and Gutierrez-Fons 2014, 9; Beck 2013, 32–33).

interpretation is rarely conclusive.[239] In this dissertation, I begin the analysis with the English-language version of the text, and if it is particularly ambiguous, I also consult the Finnish and Swedish-language versions.[240] The GDPR and the AIA are prime examples of frequently ambiguous or deliberately vague texts, [241] rendering textual interpretation alone insufficient and demanding contextual and teleological methods.

Contextual interpretation construes a provision in light of its wider context.[242] Its internal dimension encompasses a systematic interpretation of the provision's normative context, including its placement within a chapter or section, the surrounding provisions, recitals, other relevant legislation, and the general terms, concepts and principles of EU law.[243] The systematic interpretation operates on the assumption that the legislator established a coherent and consistent legal order, meaning that provisions should be interpreted in harmony with their context and without creating redundancies.[244] The external dimension of contextual interpretation encompasses analysis of the decision-making processes where the provisions were formed. [245] Hence, the external dimension scrutinises the travaux préparatoires, which carry limited weight in traditional CJEU practice but may be

239 See C-283/81 *CILFIT*, paras 18–19 and C-29/69 *Stauder v City of Ulm*, paras 2–3 and (Beck 2013, 162, 174, 189–90 and 291–93; Schermers and Waelbroeck 2001, 12–13; Menegatti 2020, 40).

240 Where discrepancies between these three language versions were identified, the German version was additionally consulted, such as in (Publication IV / Parviainen 2026).

241 For instance, regarding AIA Art. 86, the three language versions studied suggest somewhat divergent interpretations. The wording in the English version 'main elements of the decision taken' is vague and allows also for a broad reading, including the main factors that led to taking the decision. However, its Finnish ('päätöksen pääkohdista') and Swedish ('viktigaste delarna av det beslut som fattas') versions could be read as more limited, referring only to the main points of the decision taken, not to the factors that lead to it. Of ambiguous wording in the GDPR, see Art. 22(1) 'decision based solely on automated processing'.

242 See (Schermers and Waelbroeck 2001, 16–20; Lenaerts and Gutierrez-Fons 2014, 16–31; Hesselink 2011, 203–4; Neergaard and Nielsen 2011, 99; Komárek 2015, 46).

243 See (Lenaerts and Gutierrez-Fons 2014, 16; Beck 2013, 191; Schermers and Waelbroeck 2001, 16–17; Komárek 2015, 46).

244 (Lenaerts and Gutierrez-Fons 2014, 17–20). Accordingly, systematic interpretation involves, among other techniques, the use of general interpretative principles, such as *lex specialis* or *lex superior,* and interpretation by analogy or a fortiori. See (Lenaerts and Gutierrez-Fons 2014, 17; Schermers and Waelbroeck 2001, 18–19; Komárek 2015, 46).

245 (Lenaerts and Gutierrez-Fons 2014, 16–17). Some scholars refer to this external dimension as historical interpretation, see e.g., (Hesselink 2011, 202; Schermers and Waelbroeck 2001, 16; Neergaard and Nielsen 2011, 99).

increasingly relevant in resolving ambiguities in complex, technical new legislative instruments, such as the AIA. [246]

I apply the contextual interpretation throughout this dissertation.[247] First, for each provision, I examine the recitals, which assist in interpreting the meaning of the ambiguous provisions and often also enlighten on the provision's purpose.[248] As regards the interpretation of fundamental rights under the CFREU, I also note the explanations to the CFREU.[249] Second, I acknowledge the placement of the provision in the legislative instrument and its surrounding provisions.[250] Third, the general principles of EU law, particularly respect for fundamental rights and restrictive interpretation of exceptions, guide the interpretations throughout.[251] Fourth, as CJEU case law does not directly address the algorithmic recruitment context, I aim to draw reasoned inferences from the closest available precedent, where possible.[252] I also consult Advocate General Opinions, which often provide more elaborate reasoning.[253] Finally, similarly to the CJEU, I consult travaux

246 See, e.g., (Schønberg and Frick 2003, 149,155-156; Lenaerts and Gutierrez-Fons 2014, 29–31).

247 Contextual interpretation is especially important given that the relevant legislative instruments interact and at times overlap.

248 For instance, GDPR Recital 71 and AIA Recital 12 have been particularly helpful in this regard. While devoid of independent legal force, recitals assist in the interpretation of ambiguous provisions, see, e.g., cases C-215/88 *Casa Fleischhandels-GmbH*, para 31 and C-162/97 *Nilsson* and others, para 54. See also (Klimas and Vaičiukaitė 2008, 32–33).

249 This is required by TEU Art. 6(1) and CFREU Art. 52(7). Consequently, the interpretations of the CFREU should not conflict with the explanations (Lenaerts 2012, 377 and 402).

250 For instance, in the interpretation of AIA Art. 86, the placement within the instrument appears relevant, see (Publication IV / Parviainen 2026) and section 6.1.2.2 below. However, these contextual factors may sometimes also conflict with other elements of the provision, as appears to be with GDPR Art. 22, which is placed in the chapter of the data subject's rights, although in *Schufa* (C-634/21) the CJEU considered it a prohibition, see para 52. See also (Publication II /Parviainen 2022, 229–34).

251 Furthermore, the principle of effective judicial protection has formed a background to the analysis in Publication IV, and the principles of equal treatment and non-discrimination were relevant in Publication III.

252 Of analogical interpretations of case law, see also (Beck 2013, 219–20). Analogical interpretations are not always possible. For instance, extending the list of protected grounds in the Non-Discrimination Directives is not possible by analogy, see, e.g., case C-13/05 *Chacón Navas*, para 56. See also (Publication III / Parviainen 2024, 453).

253 However, the Advocate Generals' Opinions must be addressed with particular caution, as those do not necessarily represent the views of the whole court. Of the role of AG Opinions, see, e.g., (Arnull 2006, 15–16).

préparatoires selectively, primarily for the ambiguous provisions of the AIA.[254] Nevertheless, after all these interpretative steps, the provisions often remain unclear, necessitating the use of the teleological interpretation.

Teleological interpretation[255] construes a provision in light of its purpose and the broader objectives of the legislative instrument and the EU legal order as a whole (i.e. meta-purposes[256]).[257] Although it functions as a subsidiary method, applied explicitly when textual and contextual interpretations have not resolved the ambiguity,[258] teleology is frequently described as the CJEU's characteristic method.[259] The CJEU has applied teleological interpretations also to avoid unacceptable consequences of a literal interpretation[260] and to fill gaps in EU law.[261] Furthermore, it is typical in cases involving fundamental rights questions and balancing of conflicting values, principles and purposes.[262]

Teleological interpretation carries specific risks that must be acknowledged.[263] The evolution of the EU legal order has multiplied its objectives, encompassing both

254 The drafting of the AIA coincided with the writing of this dissertation, which made it easier to follow its drafting process. Of the usefulness of travaux préparatoires as regards highly technical rules, see (Schønberg and Frick 2003, 156).

255 Sometimes this is also referred to as purposive interpretation, see, e.g., (Schermers and Waelbroeck 2001, 21).

256 In prior research, the overarching purposes of the EU legal order have been framed as 'meta-purposes', see (Lasser 2004, 208; Paunio 2011, 56; Komárek 2015, 46). These meta-purposes include, for example, effectiveness, uniformity, legal certainty, and the protection of individual rights, see (Lasser 2004, 211–36; Paunio 2011, 56; Komárek 2015, 46).

257 (Maduro 2008, 3).

258 (Schermers and Waelbroeck 2001, 21; Hettne et al. 2011, 168). Ulla Neergaard and Ruth Nielsen have suggested that the teleological method may also remain implicit in CJEU's judgments (Neergaard and Nielsen 2011, 128).

259 (Hettne et al. 2011, 168; Paunio 2011, 48 and 56; Maduro 2008, 3; Lasser 2004, 229–36; Fennelly 1996, 664; Beck 2013, 289). For instance, in the CILFIT judgement (C-283/81), the CJEU appeared to require some form of contextual and teleological interpretation of all EU law as it considered in para 20 that 'every provision of Community law must be placed in its context and interpreted in the light of the provisions of Community law as a whole, regard being had to the objectives thereof and to its state of evolution' at the time of applying the provision.

260 (Schermers and Waelbroeck 2001, 21–29; Hettne et al. 2011, 168–69; Fennelly 1996, 674). These may include, for instance, conflicts with the purpose or general scheme, see (Beck 2013, 189).

261 (Neergaard and Nielsen 2011, 127). See also case C-634/21 *Schufa*, para 52 and AG Pikamäe's opinion in that case, para 31.

262 See, e.g., (Beck 2013, 280; Tecqmenne 2024, 255 and 270; Raitio 2013, 209).

263 See, e.g., (Neergaard and Nielsen 2011, 118–19; Maduro 2008, 5–6).

internal market and increasingly social aims.[264] Where the objectives point in different directions, the interpreter may selectively invoke the purposes to support a preferred interpretation.[265] Hence, some scholars have argued that predicting outcomes of teleological interpretations is difficult, which may negatively affect legal certainty.[266] Teleological interpretations have also raised concerns of judicial activism[267] or judicial law-making that lacks legitimacy.[268] In contrast, some scholars argue that where the wording is ambiguous, the legislator has deliberately left the matter for the CJEU to decide. [269] While noteworthy, these risks do not eliminate the utility of teleological interpretation.[270]

In this dissertation, I use teleological interpretations to supplement textual and contextual interpretations where ambiguity persists.[271] It operates most straightforwardly in relation to the Non-Discrimination Directives, whose purpose, combating discrimination and giving effect to equal treatment, is internally consistent.[272] The dual purpose of the GDPR and the market-integration emphasis of the AIA, described in section 1.3.3, complicate the teleological interpretation of

264 See, e.g., TEU Arts. 2, 3 and 6. For a recap of the developments, see, e.g., (Neergaard and Nielsen 2011, 114–16). In the controversial *Viking* (C-438/05) and *Laval* (C-341/05) cases, where competing economic and social objectives were prominent, the CJEU prioritised the economic objectives. However, since the entry into force of the Lisbon Treaty and the CFREU's enhanced role, social objectives have appeared to gain greater prominence. This shift is also visible in the field of labour law, see, e.g. (Menegatti 2020, 41–42).

265 (Beck 2013, 176–78). For instance, through teleological interpretation, the CJEU has recognised certain fundamental rights as directly applicable in private relationships, generating rights and obligations not expressly provided for in EU secondary law. See, e.g., joined cases C-596/16 and 570/16 *Bauer* and C-648/16 *Max Planck* and (Tecqmenne 2024, 255 and 270–72). Cf. in C-176/12 *Association de médiation sociale*, the CJEU stuck to a stricter textual reading and came to the conclusion that CFREU Art. 27 was not a source of rights and obligations in private proceedings.

266 See, e.g., (Tecqmenne 2024, 267–68).

267 See, e.g., (Neergaard and Nielsen 2011, 118–19; Maduro 2008, 5–6; Muir et al. 2013, 3; Tridimas 2013, 215–21). For instance, cases C-144/04 *Mangold* and C-555/07 *Kücükdeveci*, where the general principle of equal treatment on the ground of age was deemed to have a horizontal direct effect, raised sharp criticism of the CJEU's alleged judicial activism.

268 See (Tecqmenne 2024, 271–72) criticising cases C-596/16 and C-570/16 *Bauer* and case C-648/16 *Max-Planck* for constituting judicial law-making.

269 See, e.g., (Beck 2013, 161, 172–73; Arnull 2006, 620–21; Maduro 2008, 6–7).

270 Several arguments in support of teleological interpretations have been presented in prior scholarship: they promote the uniform application of EU law across the Member States' diverse linguistic and legal traditions, provide normative guidance for national courts in future cases, and enable the adaptation of older and general norms to novel situations. See, e.g., (Maduro 2008, 6–7; Beck 2013, 172–73; Fennelly 1996, 664–65).

271 As an example, see (Publication II /Parviainen 2022, 230–31).

272 See RED Art. 1, EED Art. 1 and GED Art. 1.

those instruments, since the competing objectives may support diverging interpretations. Nevertheless, when interpreting these instruments teleologically, I aim to balance competing objectives and provide justification for my choices.[273]

Since the protection of fundamental rights is among the purposes of all the central EU legislation examined in this dissertation, teleological[274] interpretations may often involve fundamental rights protective reasoning.[275] The difficulty is that there is seldom only one fundamental right or freedom involved, and the CFREU does not establish any explicit hierarchy among rights.[276] As discussed in section 1.3.2, the most relevant rights include job applicants' rights to data protection[277], non-discrimination,[278] and effective remedies,[279] alongside employers' freedom to conduct business.[280] Where these rights compete in an interpretative situation, I conduct a case-by-case balancing of those competing rights,[281] seeking an interpretation that minimises interference with all the rights involved[282] and respects

273 Of these requirements, see also (Lenaerts and Gutierrez-Fons 2014, 33; Beck 2013, 176–78).

274 As was mentioned above, fundamental rights respecting interpretations are also required as part of the contextual interpretations, as the general principle of respect for fundamental rights should be noted.

275 Given the purposes of the legislation examined, the Non-Discrimination Directives are the most likely to trigger a fundamental rights protective interpretation. The second is the GDPR, where fundamental rights are also prominent, although not the only aim. Of these three rule sets, the interpretation of the AIA is the most likely to emphasise the internal market goals over fundamental rights, given the importance of the former among its purposes.

276 See (Lenaerts 2012, 392–93; Koukiadaki 2019, 126). Nevertheless, no limitations are allowed on Title I rights, see, e.g., (Koukiadaki 2019, 120; Lenaerts 2012, 392).

277 CFREU Art. 8.

278 CFREU Arts. 20, 21 and 23.

279 CFREU Art. 47.

280 CFREU Art. 16. At times, also third parties' right to property or protection of personal data might be at stake. This could be the case, for example, if providing an explanation about ARS's decisions would reveal personal data of other applicants or ARS providers' trade secrets. See also GDPR Recital 63.

281 See also CFREU Art. 52(1). On balancing, see also (Alexy 2002, 47–48, 50, 67 and 101–7). However, the balancing is by no means unproblematic, see, e.g., (Tsakyrakis 2009; Koukiadaki 2019, 127–30; Harbo 2010, 169–71; van der Sloot 2016).

282 The proportionality analysis applied follows the structured approach established in CJEU case law, assessing whether any limitation on a fundamental right pursues a legitimate aim and is suitable, necessary and proportionate stricto sensu (i.e. does not impose an excessive burden on the individual). See, e.g., case C-92/09 *Volker und Markus Schecke and Eifert*, paras 65–87 and C-414/16 *Egenberger*, paras 68–69 and 80–81. The proportionality principle is also reflected in the analysis of legitimate interests (see section 5.2.2 below) and indirect discrimination (see section 5.2.1.2 below). Of the use of proportionality analysis to balance competing rights, see, e.g., (Koukiadaki 2019, 126–27; Harbo 2010; Alexy 2002, 67).

their essence[283]. In this balancing exercise, I note the vulnerability of job applicants vis-á-vis employers using ARS. Such vulnerability is recognised in the data protection scholarship[284] and the European Data Protection Board's (EDPB) guidance,[285] as well as some labour law scholarship[286]. Although this vulnerability does not automatically tip the balance in favour of applicants, it carries weight in the proportionality assessment. Nevertheless, I aim to find an interpretation that optimises all the rights involved.[287]

1.4.3 Systematisation

The objectives of this dissertation expressly include producing a comprehensive and systematised account of EU legislation that constrains and shapes employers' use of ARSs.[288] Furthermore, systematisation also supports the analysis of the job applicants' legal safeguards. Hence, systematisation is necessary to meet the objectives.

First, I had to develop the conceptual framework underpinning the legal analysis and systematisation.[289] Statutory definitions in this field are often ambiguous,[290] their interpretation continues to evolve,[291] and in some cases, they are absent altogether, necessitating the development of certain concepts specifically for this dissertation.[292] Chapter 2 introduces the key concepts used in this dissertation. Where EU legislation

283 For instance, the impossibility to exercise a right could constitute an interference with its essence, see (Brkan 2019b, 882). See also (Brkan 2018) and section 1.3.2 above.

284 See, e.g., (Malgieri 2023, 138).

285 See also (EDPB 2020c, 9; 2020b, 9).

286 See (Lacková 2022, 73–74). While not all the vulnerabilities and problems existing during the employment relationship are present in the pre-contractual stage, for instance, the imbalance of power typically exists already in the recruitment phase. Of the vulnerabilities in general, see, e.g., (Davidov 2016a, 34–54).

287 See also (Alexy 2002, 67; Harbo 2010, 166). For instance, in (Publication II /Parviainen 2022, 241–42), I proposed an interpretation that permits employers to utilise ADM in certain, particularly limited situations, subject to safeguards designed to preserve the fundamental rights of job applicants.

288 See section 1.2 above.

289 Although presented here in the systematisation section, the conceptual framework also supports the interpretations discussed above in section 1.4.2.

290 See, e.g., AIA Art. 3, point 1 and GDPR Art. 22. Of causes of ambiguity in general, see, e.g., (Beck 2013, 56–58) and of the open texture of law and its effects, particularly in the context of the AIA, see also (Lanamäki et al. 2025).

291 For instance, the European Commission's guidelines on the concept of AI systems that guide the interpretation of the AIA's definition were given when writing this synthesis, see (European Commission 2025d). Further, the concept of automated decision-making has developed in the CJEU's case law during this project; see, e.g., C-634/21 Schufa.

292 See sections 2.3, 2.4 and 2.6 below.

or CJEU jurisprudence provides definitions, those are adopted.[293] Where statutory or judicial definitions are absent, working definitions are proposed based on relevant EU law and scholarship.

The main systematisation effort is the organisation of the relevant EU legislation into the framework of key legal parameters for the use of ARSs. Reflecting the objectives of this dissertation, the framework serves two purposes: to provide an analytical foundation for the evaluative analysis conducted in Chapter 6, and to function as a heuristic structure for navigating the complex normative landscape governing ARS use. In line with the limitations of this dissertation, the legal parameters included in the framework were selected because they directly affect employers' use of ARSs involving AI or algorithmic decision-making and are relevant to job applicants' protection against data protection infringements and discrimination.[294] Given the breadth of the regulatory landscape and the more detailed legal dogmatic analysis of specific provisions in Publications II-IV, the framework offers a systematised overview rather than an exhaustive analysis of each parameter.

The framework of key legal parameters presented in Chapter 5 and Annex I is not built upon any existing normative taxonomy,[295] as no such taxonomy appeared

[293] As regards a statutory definition of an AI system, see section 2.2. However, the statutory definitions are often open to various interpretations, and Chapter 2 aims to explain the interpretation utilised herein.

[294] See sections 1.3.1 and 1.3.3. Since the employer - job applicant relation is at the core of this dissertation, the framework does not cover employers' obligations vis-à-vis other parties and draws primarily on EU secondary legislation. For instance, trade secrecy, IPR and product liability norms are excluded from the framework as independent legal parameters due to the framework's focus on the employer-job applicant relation and the associated data protection and non-discrimination risks. Of the limitations of the Product Liability Directive (PLD), i.e. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (Text with EEA relevance) in the algorithmic recruitment context, see also (Grozdanovski 2025, 20–21).

[295] An instructive existing taxonomy is *Anthony Ogus's* classification of regulatory instruments according to the degree of state intervention required, noting also their legal form and the degree of constraint they impose. In the field of social regulation, to which also the recruitment context could fall, Ogus distinguishes the following strategies proceeding from low to high intervention: (1) information regulation, that demands certain disclosures, (2) 'private' regulation that imposes obligations that only those individuals for whose benefit they have been created can enforce, (3) economic instruments, that prompt desirable behaviour by financial incentives, (4) command-and-control regulation where standards are imposed and backed by criminal sanctions, and (5) prior approval, which prohibits an activity without a license or authorization. See (Ogus 2004, 4–5).

to exist, onto which the key legal parameters for ARS use could neatly map.[296] Therefore, I developed the categorisation inductively from the legal material itself.[297] The categorisation reflects the structural and functional characteristics of the relevant provisions. The resulting framework of key legal parameters is organised along two dimensions, each reflecting a distinct systematisation logic.

The first dimension classifies legal parameters by the type of recruitment system, illustrating how different systems activate distinct legal parameters. By the type of recruitment system, I refer not only to the underlying technology but also to the extent of human involvement in decision-making, as both factors are relevant in determining the applicable legal parameters. Thus, three main system categories are distinguished: all ARSs, AI systems,[298] and systems involving automated decision-making.[299] This classification reflects the risk-based regulatory logic of the AIA[300] and certain provisions of the GDPR[301], where the requirements applicable to a system depend on its risk level.[302]

The second dimension classifies the legal parameters within each system category according to their normative characteristics. The legal parameters are grouped into four categories: *bans, obligations, specific duties and actionable*

296 This might be partly due to the breadth and variety of the EU legislation considered. The framework of key legal parameters combines different types of regulatory instruments, including more risk-based and rights-based legislation. Of the differences between the AIA and the GDPR in this regard, see, e.g., (Gellert 2021; Leufer and Hidvegi 2023; Ebers 2024).

297 *Jan M. Smits* has noted that 'it is to the person making the systematisation to decide which rules should be tied together under which principles and policies', see (Smits 2017, 217).

298 High-risk AI systems and high-risk AI systems that assist in individual decision-making are subcategories of AI systems. See sections 2.2, 5.1 and Appendix I.

299 For the different types of systems, see also sections 2.2-2.4 and 5.1 below.

300 See AIA Recitals 26–27 and (Smuha and Yeung 2025, 236–45). However, in prior scholarship, it has also been questioned whether the AIA adopts a truly risk-based approach, see, e.g., (Ebers 2024).

301 For instance, the rules on data breach notifications (Arts. 33–34) and data protection impact assessments (Arts. 35-36) adopt a risk-based approach, although the GDPR could primarily be seen as a rights-based instrument. GDPR Art. 22 could also be seen as risk-based, with the threshold it sets for the decisions that trigger it. See also (Leufer and Hidvegi 2023).

302 Of the differences between risk- and rights-based approaches in these instruments, see (Gellert 2021; Leufer and Hidvegi 2023; Ebers 2024). However, the rights-based provisions of the GDPR, the Non-Discrimination Directives and the Pay Transparency Directive (PTD) (i.e., Directive (EU) 2023/970 of the European Parliament and of the Council of 10 May 2023 to strengthen the application of the principle of equal pay for equal work or work of equal value between men and women through pay transparency and enforcement mechanisms) are visible in the legal parameters applicable to all ARSs.

rights.[303] These categories are differentiated by four factors: their normative intensity and rigidity, normative target, scope and realisation mechanism. Normative intensity and rigidity capture the strictness or permissiveness of the parameters[304] and the level of flexibility they allow[305]. Normative target distinguishes parameters that impose duties on employers or set requirements for the systems used from those that confer entitlements on job applicants. Scope refers to the breadth of algorithmic recruitment situations to which the parameter applies. Finally, the realisation mechanism distinguishes parameters that apply in all cases from those that depend on the job applicant's active invocation or enforcement.

Accordingly, *bans* represent legal limits that may not be transgressed. These are further divided into *absolute bans,* which admit no exceptions, and *qualified bans,* which allow derogations under certain conditions. Second, *obligations* encompass general, often system-level responsibilities that govern either the ARS itself or its use.[306] Third, *specific duties* refer to concrete requirements imposed on employers that demand their proactive measures and arise due to the nature or type of the system deployed.[307] Finally, *actionable rights* comprise legal entitlements that job applicants may invoke in connection with ARS use, the realisation of which depends on their active exercise or enforcement. Nevertheless, the boundaries between the

303 See section 5.2 below and Appendix I. In *Anthony Ogus's* classification, all these categories would mostly be command-and-control regulation, with the distinction that there are only administrative sanctions, and no criminal sanctions, at the EU level. However, the obligations and specific duties also contain some information regulation, often backed up by administrative sanctions. The actionable rights also resemble some elements of private regulation as depicted by Ogus's classification, as they require enforcement by individuals. Yet, none of the Ogus's categories fit perfectly into this context. Cf. (Ogus 2004, 5, 150–51, and chapters 7, 8, 9 and 12).

304 E.g. whether the provision is an absolute prohibition (e.g. AIA Art. 5(1)(a)) or does it contain exceptions (e.g. GDPR Art. 22).

305 I.e. is the provision formulated as a precise rule (GDPR Art. 13) or more as an open-textured standard (GDPR Art. 5).

306 The obligations also contain general legal boundaries that curtail ARS use. However, in accordance with the limitations of the framework, general obligations that do not directly affect the ARSs or their use, such as the obligation to maintain records of processing activities under GDPR Art. 30, are not included in the framework.

307 The specific duties encompass only legal parameters that are triggered especially when using ARSs, and not generally for recruitment processes (see section 5.2.3 below). Hence, the general legal parameters governing recruitment processes are not covered in the duties section, such as the PTD's general obligations on pay transparency. Similarly, the Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (CSDDD) is not included even though it requires certain larger companies (see CSDDD Art. 2) to conduct risk-based human rights due diligence (see CSDDD Arts. 7 to 16), where also ARSs should be included.

categories remain porous.[308] Certain provisions could plausibly fall into multiple categories, depending on their interpretation.[309] Chapter 5 elaborates on these categories and the criteria that differentiate them, further explaining the interpretations that have led to the chosen categorisation.

The framework of key legal parameters provides the analytical foundation for addressing the second research question in Chapter 6, as these parameters form the basis of job applicants' legal safeguards as well. However, considering the more practical objective of assisting job applicants and their representatives in understanding and enforcing job applicants' rights, the framework of key legal parameters alone remains too abstract. To more clearly present the legal safeguards available to job applicants, Chapter 6 analyses them using a safeguards-based typology that builds on prior scholarship, distinguishing ex-ante preventive safeguards from ex-post reactive safeguards.[310] However, not all the safeguards sit comfortably within that binary. For instance, the right to explanation could incentivise employers to refrain from using ARSs that resist all explanations, although the right to explanation requires job applicants to invoke it actively and, in that sense, operates as a reactive safeguard.[311] Therefore, a third intermediate category of informational safeguards that simultaneously supports prevention and reaction is warranted. Treating informational safeguards as either purely preventive or purely remedial would obscure their role in the enforcement chain, since they could affect both the effectiveness of ex-ante safeguards and the practicability of ex-post safeguards. The relevant EU legislation is accordingly mapped onto three categories: preventive, informational, and remedial safeguards, which constitute the analytical structure for Chapter 6.

308 For instance, purely based on its wording, GDPR Art. 22 would have been an obligation. However, according to the CJEU (*Schufa* C-634/21, para 52), GDPR Art. 22 should be framed as a prohibition. Simultaneously, some provisions, such as GDPR Art. 6, have now been categorised as obligations, although they could also have been framed as prohibitions, see also (Publication I / Viljanen and Parviainen 2022, 2–3).

309 For instance, viewed through the Hohfeldian framework of legal relations, actionable rights could be alternatively framed as more general duties of the employers. These duties arise, at the latest, when job applicants exercise their rights and must therefore be noted when ARSs are used. This reflects the Hohfeldian principle that every right held by one party implies a correlative duty on the part of another (Hohfeld 1913, 30–32).

310 See, e.g., (Shavell 1993, 257–58; Suksi 2020, 4; Smuha 2024a, 254).

311 See AIA. Art. 86 and GDPR Art. 15(1)(h) and section 6.1.2.2.

1.5 Sources, tools and structure

In this dissertation, the primary sources are EU secondary law, particularly the GDPR, the AIA and the Non-Discrimination Directives.[312] The CFREU and the general principles of EU law inform their interpretation throughout, and the CFREU also plays a more direct and independent role, particularly through its provisions having horizontal direct effect.[313] Recitals[314] and the explanations to the CFREU are also examined where relevant.[315] Where national law examples are needed, I draw upon Finnish legislation and case law.[316]

As discussed in section 1.4.2, CJEU case law is an important source, and I also examine Advocate General Opinions that often provide more elaborate reasoning.[317] Since case law directly addressing AI and algorithmic decision-making remains limited, EDPB guidance[318] and the Commission's guidelines on the application of the definition of an AI system and on prohibited AI practices[319] serve as significant interpretative aids. Notwithstanding their non-binding nature, these instruments indicate how the relevant provisions may be applied in practice. Preparatory works are consulted selectively.[320]

312 See sections 1.1.1, 1.3 and 1.4.1 above. In addition to these, there are a number of other secondary law instruments that have been reviewed, and of those, the PTD is also included in the framework of key legal parameters. As regards the market surveillance of AI systems, the Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance), hereinafter 'Market Surveillance Regulation' is to be noted.

313 This has been discussed in particular in (Publication III / Parviainen 2024), in Chapters 5 and 6 below, and briefly in (Publication IV / Parviainen 2026).

314 Of the nature and role of recitals, see footnote 248 above.

315 TEU Art. 6(1) and CFREU Art. 52(7) require that the Explanations relating to the Charter of Fundamental Rights (2007/C 303/02), drawn up to guide the interpretation of the CFREU, are 'given due regard'. The Explanations themselves state that 'although they do not as such have the status of law, they are a valuable tool of interpretation to clarify the provisions of the Charter' (p. 17). However, the CJEU has only selectively relied on the Explanations, see, e.g., cases C-193/17 *Cresco Investigations* compared to C-176/12 *Association de médiation sociale* and (Muir 2019, 214; Tecqmenne 2024, 262 and 265).

316 See especially (Viljanen and Parviainen 2022, 2).

317 See footnote 253 above.

318 To the extent that the EDPB has endorsed the documents of the former Article 29 Working Party (WP29), those have also been analysed and noted when interpreting the GDPR. See (EDPB 2018a).

319 See, e.g., (European Commission 2025c; 2025d).

320 See section 1.4.2.

Beyond these sources, this dissertation draws on legal scholarship on EU law, labour law, data protection law, non-discrimination law and AI regulation, as well as technical and non-legal scholarship necessary to understand how ARSs operate and what risks they pose. Computer science research[321] and human resources literature[322] primarily serve a pre-interpretative function, providing the factual and technical foundation for the legal analysis.[323] When examining available ARSs and their characteristics, I also utilised information from providers' websites[324] and prior reports and research regarding those systems[325]. In accordance with the limitations discussed in section 1.3.3, I do not study international law, common constitutional traditions of the Member States, or soft law in detail.[326]

In relation to acquiring sources, I experimented with several AI applications designed for literature reviews, such as Scite[327], Scispace[328], and Researchrabbit[329], but did not use them systematically. Further, I also tested Claude[330] to help find relevant scholarly sources. However, I used these AI applications primarily to double-check that I had not missed any relevant sources in my traditional searches conducted mainly through library-provided databases, Google Scholar, and EUR-

321 See, e.g., (Bowman 2023; OpenAI 2023b). Computer science research papers and technical reports are utilised, especially in Chapter 3 of this synthesis.

322 See, e.g., (Budhwar et al. 2023; Horodyski 2023; Li et al. 2021; Ore and Sposato 2022). The AIAAIC Repository was also used as a resource for finding real-life incidents regarding ARS use, see (AIAAIC 2025).

323 See section 1.4.2 and Chapter 3 below. When building understanding about the risks and operations of different kinds of ARSs, for instance, the following sources were consulted (Bommasani et al. 2021; Dale 2021; Hacker et al. 2023; 2025).

324 See, e.g., (Jobilla 2025; Oleeo 2025; CVViz 2023; Zoho Recruit 2025; pymetrics 2023; HireVue 2023; Arctic Shores 2025; Sapia.ai 2025; Jotform 2025; Humanly 2025; JOBMA 2025; Metaview 2025).

325 See, e.g., (Bogen and Rieke 2018; Sánchez-Monedero et al. 2020).

326 In EU labour law, the EU-level agreements between trade unions and employers' associations, as well as the EU's targets and recommendations that aim to shape Member States' labour market policies, could be important, see (Davies 2012, 5, 35–39). The importance of soft law is also highlighted in the AIA, where standards play a significant role (AIA Arts. 40, 42–43) and have legal effects, see, e.g., (Bygrave and Schmidt 2024, 11; Veale and Zuiderveen Borgesius 2021, 104–6). See also case C-588/21, *Public.Resource.Org and Right to Know v Commission and Others*, paras 65-87. However, AIA-based standards are still in preparation (European Commission 2026), and other standards are mostly not freely accessible. For instance, the ISO/IEC 42001:2023 Standard Information Technology – Artificial Intelligence – Management System costs about 250 euros.

327 (Scite.ai 2025).

328 (Scispace.com 2025).

329 (ResearchRabbit.ai 2025).

330 (Anthropic PBC 2026).

lex.[331] In addition to traditional Google searches, I also used ChatGPT to find practical examples of currently available algorithmic recruitment systems. Furthermore, I briefly tested NotebookLM[332] and Legora[333] as auxiliary tools to generate preliminary summaries of source materials, helping identify the most relevant sources for detailed analysis. In any case, I have critically reviewed and analysed all relevant source materials to ensure accuracy.

I have used AI applications for language checking and targeted editing. The language of Publications I and III was checked with Grammarly before final submission. When preparing this synthesis and Publication IV, I have utilised Grammarly[334] and, on occasion, ChatGPT[335] or Claude to check language and improve the clarity of the text I have authored myself.[336] However, when writing Publication II, no separate AI applications were used.[337] Recognising the potential biases and limitations inherent in AI applications, I have critically assessed all AI-generated suggestions.[338] Importantly, I have not relied on AI-generated content for substantive arguments, analysis or conclusions.

This dissertation is organised into seven chapters. Following this introduction, Chapter 2 introduces the key concepts used throughout this dissertation. Understanding the legal constraints imposed on AI and algorithmic decision-making, and the effectiveness of job applicants' safeguards, requires a grounded account of how such systems are built and deployed. Therefore, Chapter 3 provides an overview of the typical use cases of algorithmic recruitment systems, their lifecycle and technological basis, providing the technical grounding necessary before the legal analysis can proceed. Chapter 4 briefly presents the individual publications comprising this dissertation. I review and analyse their findings in more detail throughout this synthesis, where they directly inform the analysis. Chapter 5 presents the framework of key legal parameters for ARS use, analyses how EU legislation

331 Nevertheless, the growing number of academic papers on this topic has increased the risk that some important points discussed in earlier research may have gone unnoticed. To mitigate this risk, I have set up alerts for new publications across various databases and have regularly checked the most important journals.

332 (NotebookLM.google 2025).

333 (Legora.com 2025).

334 (Grammarly.com 2025).

335 (Chatgpt.com 2025).

336 For instance, *Brent Mittelstadt et al.* have presented that LLMs should be used only as 'zero-shot translators: to convert accurate source material from one form to another' (Mittelstadt et al. 2023, 1830).

337 Traditional language correcting functions in Word were also used in writing Publication II, which might have included some AI-based functionalities.

338 Practical exploration with the AI tools provided also empirical insights into their advantages and limitations.

constrains and shapes the use of ARS, and discusses the implications for employers. Chapter 6 examines the legal safeguards EU legislation provides to protect job applicants' rights to data protection and non-discrimination when AI and algorithmic decision-making are used in recruitment, addresses the shortcomings of these legal safeguards using an LLM-based recruitment system as a case example, and concludes with a summary of the proposals put forward throughout this dissertation to strengthen those safeguards. Finally, Chapter 7 discusses the main contributions of this dissertation, their potential impact, and directions for further research.

2 Key Concepts

2.1 Recruitment

EU law does not contain an explicit statutory or judicial definition for recruitment.[339] Nevertheless, defining recruitment is essential, as the legal constraints applicable to a given activity may differ depending on whether that activity qualifies as recruitment or falls outside its scope. The qualification as recruitment can influence, for instance, the validity of consents for processing personal data or making automated decisions,[340] and the classification of certain systems as high-risk AI systems.[341]

Although EU law does not provide an explicit definition of recruitment, several pieces of legislation refer to it,[342] and the CJEU has given numerous judgments addressing various aspects of recruitment processes. The following stages of the recruitment process are recognised in EU legislation or case law: recruitment policies,[343] (targeted) job advertisements,[344] analysis and filtering of job applications,[345] selection criteria and recruitment conditions,[346] applicants'

339 This is by no means unprecedented, as despite its importance, EU legislation does not contain a unified definition of worker either, see, e.g., (Menegatti 2020, 29). However, CJEU's interpretations of the concept have aimed to create an EU concept of 'worker'.

340 (EDPB 2020c, 9; WP29 2018b, 7).

341 AIA Article 6 and Annex III, point 4(a), according to which 'AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates' count as high-risk AI systems.

342 See, e.g., AIA Annex III, point 4(a), RED Art. 3, EED Art. 3 and GED Art. 14, Regulation on freedom of movement for workers Arts. 2 and 3.

343 See, e.g., cases C-54/07 *Feryn,* paras 29–34, C-81/12 *Asociatia Accept,* paras 45–49, and C-507/18 *Associazione Avvocatura per i diritti LGBTI,* paras 42–43.

344 AIA Annex III, point 4(a) and PTD Art. 5.

345 AIA Annex III, point 4(a).

346 See RED Art. 3, EED Art. 3 and GED Art. 14. These could include, for instance, language requirements (e.g. C-379/87 *Groener*), certification requirements (C-281/98 *Angonese* and C-317/14 *Commission v. Belgium*), and age limits (C-419/92 *Scholz*, C-278/03 *Commission v Italy* and C-371/04 *Commission v Italy*).

evaluation[347] and acceptance of job offers[348]. In its non-discrimination rulings, the CJEU has interpreted the concept of 'conditions for access to employment' rather broadly, encompassing situations where no public tender or formal selection procedure is open, but where the circumstances nonetheless affect certain job applicants' factual possibility of being employed.[349] Accordingly, at least the above-listed stages likely qualify as recruitment under EU law. However, the list is not exhaustive, and stages not yet explicitly recognised in EU law may still qualify as recruitment where they affect applicants' factual access to employment in a comparable manner.[350]

Understanding what falls within the scope of recruitment under EU law may be informed by two further bodies of literature. First, general human resources (HR) literature provides a much more granular framework. In HR literature numerous stages of the recruitment and selection process[351] have been identified including activities such as organisational diagnostics, analysing the necessity of the open position, job analysis, drafting job descriptions and job specifications, determining selection criteria, creating application forms, choosing methods for reaching candidates and advertising the position, planning interview and assessment procedures, receiving applications, shortlisting applicants, conducting interviews, psychometric testing, attending an assessment centre, checking references, performing medical assessments, preparing a training and educational plan for selected candidates, deciding employment terms, making job offers, conducting induction, monitoring the performance of successful candidates, and establishing feedback mechanisms.[352]

347 AIA Annex III, point 4(a).

348 The right to accept job offers is included in the EU primary law's founding principle of freedom of movement for workers, see Art. 3(2) TEU and Arts. 26 and 45–46 TFEU. It is also closely linked to CFREU Art. 15 on the freedom to choose an occupation and the right to engage in work.

349 C-81/12 *Asociatia Accept*, paras 44–45. Stages preceding public selection procedures have been considered as conditions for access to employment also in cases C-54/07 *Feryn*, and C-507/18 *Associazione Avvocatura per i diritti LGBTI*, paras 42–43.

350 Furthermore, it is possible that Member States view the recruitment process also more broadly, if such an approach better protects job applicants. See, e.g. AIA Art. 2(11), RED Art. 6, EED Art. 8 and GED Art. 27. For instance, the Finnish Supreme Court has deemed that recruitment typically refers to actions that establish an employment relationship, including measures ranging from preparation of the recruitment process to selecting a candidate (KKO:2025:50, para 16).

351 In human resources literature, recruitment and selection are often considered separate functions, see, e.g., (O'Meara and Petzall 2013, 6–11; Reynolds and Dickter 2017, 856). However, the use of technology in the process might ideally make those more closely integrated, see e.g., (Reynolds and Dickter 2017, 856).

352 See e.g., (O'Meara and Petzall 2013, 7–11; Stone et al. 2013; Elearn 2009; Barber 1998).

Second, prior research on algorithmic hiring has proposed a more condensed four-stage model that distinguishes between *sourcing, screening, interviewing*, *and selection.*[353] The *sourcing* stage aims to identify potential applicants who may be suitable for the position and encourage them to apply.[354] The sourced applicant pool is then *screened* using various tools, tests and screening criteria to discover the most qualified and suitable applicants, who are invited to an interview.[355] In the *interview* stage, applicants' suitability for employment is further assessed.[356] Finally, the recruitment process concludes with the *selection* stage, where the employer determines the most suitable candidate and makes a final recruitment decision.[357]

This four-stage model is suited to analysing where algorithmic systems intervene. However, to clearly reflect all the stages of the recruitment process recognised under EU law, a broader definition is required. Accordingly, for the purposes of this dissertation, the term *recruitment* is deemed to encompass the entire process of hiring an employee by the employer, including the determination of recruitment policies and practices, candidate sourcing, screening, interviewing, selection, and the conclusion of an employment contract with the chosen applicant.[358] Since recruitment policies and practices are explicitly covered, the use of ARSs is part of recruitment even when no particular position is open.[359]

In practice, recruitment processes are diverse and tailored to the specific open position, the employer's needs, and the prevailing labour market conditions, among other factors.[360] Not every recruitment process necessarily comprises all the stages, and those may also be intertwined, overlapping or occur in a different order.

353 (Raghavan et al. 2019, 3; Bogen and Rieke 2018, 13). See also *Alessandro Fabris et al*., who have included the evaluation of the employees chosen into the four stages of the recruitment process (Fabris et al. 2024, 3).

354 (Fabris et al. 2024, 3; Bogen and Rieke 2018, 14). This stage might also be termed 'recruitment' or 'attraction', see, e.g., (Breaugh 2013; Chapman and Mayers 2018; Reynolds and Dickter 2017, 856–58).

355 (Fabris et al. 2024, 4; Chen 2023, 140–41; Black and van Esch 2020, 220; Sivathanu and Pillai 2019, 459; Cohen 2019, 63; Bogen and Rieke 2018, 26).

356 (Macan 2009, 203; Levashina et al. 2014, 241).

357 (Bolander and Sandberg 2013, 302; Bogen and Rieke 2018, 39).

358 In previous research, for example, *Eva Lacková* has considered that the process starts when the employer announces the start of the selection procedure and ends when the selections are made, and the candidates are informed of the decision (Lacková 2022, 72).

359 See also CJEU cases C-54/07 *Feryn* and C-81/12 *Asociatia Accept*.

360 (Orlitzky 2009; Breaugh 2013; Lievens and Chapman 2019, 140).

2.2 Artificial intelligence (AI) system and high-risk AI system

EU law provides a statutory definition of artificial intelligence systems (hereinafter AI systems).[361] Thus, any mention of AI[362] in this dissertation pertains to AI systems as defined in AIA Article 3, point 1 and interpreted in line with the Commission's guidelines on the definition of an artificial intelligence system[363]. In AIA Article 3, point 1, an AI system is defined as '[1] *a machine-based system* [2] *that is designed to operate with varying levels of autonomy and* [3] *that may exhibit adaptiveness after deployment and* [4] *that, for explicit or implicit objectives* [5] *infers, from the input it receives, how to generate outputs* [6] *such as predictions, content, recommendations, or decisions* [7] *that can influence physical or virtual environments*'.[364] As outlined in the Commission's guidelines, an AI system must exhibit these seven main elements at some point in its lifecycle, although they do not need to be present continuously.[365]

The first criterion, that the system is machine-based, is fulfilled by computer-based systems.[366] Second, to meet the autonomy criterion, the system should operate with some level of autonomy[367], meaning a 'reasonable degree of independence of actions'[368]. In the Commission's guidelines, the autonomy criterion is closely tied to inference, which suggests that merely automating tasks based on fully human-

361 See AIA Art. 3, point 1.

362 The term 'Artificial Intelligence' appears to date back to 1955 Dartmouth, see (McCarthy et al. 1955). AIA Recital 12 depicts the difficulties in defining artificial intelligence in legal or technological terms. A broad definition could apply better to future developments, but a precise and clear definition would provide more legal certainty, while risking becoming obsolete quickly. See also (Wang 2019, 7–8; Schuett 2023, 4; 2019, 2). Cf. In public discourse, artificial intelligence is commonly understood as a technology that enables machines to perform tasks which, if performed by humans, would require intelligence, see, e.g., (Lea 2024, 58; Breidbach 2024, 1; Mitchell 2023).

363 Based on AIA Art. 96(1)(f), the Commission has given guidelines on the application of the definition of an AI system, which aim to assist in determining whether a system constitutes an AI system (European Commission 2025d, 1).

364 The numbering of the key elements as added in (European Commission 2025d, 2). This definition aligns closely with those of international organisations working on AI, such as the OECD and COE. See AIA Recital 12, (OECD 2024) and Article 2 of the Council of Europe Framework Convention on Artificial Intelligence. However, it has been criticised, among other reasons, for being too broad, see e.g., (Hacker 2024a, 3; Ebers 2024, 12).

365 (European Commission 2025d, 2).

366 See AIA Recital 12 and (European Commission 2025d, 2–3). Similarly also (Voigt and Hullen 2024, 5).

367 AIA Art. 3, point 1, does not set any specific threshold for autonomy.

368 AIA Recital 12 and (European Commission 2025d, 3–4).

defined rules does not suffice to fulfil the autonomy criterion.[369] Third, the criterion requiring adaptiveness after deployment appears optional based on its wording ('may').[370] Fourth, AI systems operate towards explicit objectives (i.e., clearly stated and developer-encoded) or implicit objectives (i.e., deduced from the system's behaviour or underlying assumptions).[371]

The fifth criterion, which involves inferring from the input the system receives how to generate outputs, could be the most important when assessing some borderline cases. The wording of AIA Article 3, point 1, and AIA Recital 12 suggest that two types of inference could fulfil this criterion. On the one hand, the capability to infer comprises 'the process of obtaining the outputs […] which can influence […] environments'. On the other hand, it encompasses the 'capability of AI systems to derive models or algorithms, or both, from inputs or data'.[372] Hence, inference can occur during either the use phase[373] or the development phase[374] of the system.[375] The capacity to infer 'transends basic data processing' since it enables the systems to learn, reason or model.[376] This capacity distinguishes AI systems from traditional software or rule-based automation, which function solely on explicitly defined instructions and do not involve learning, reasoning or generating outputs beyond pre-programmed rules.[377]

The sixth criterion refers to the various functions that AI systems can perform, providing example output categories such as predictions, content, recommendations, or decisions.[378] Predictions are forecasts of unknown outcomes derived from known data provided to the system.[379] Content signifies new material generated by the system.[380] Recommendations propose specific actions, and decisions are defined as 'conclusions or choices' that the system has made.[381] Finally, the seventh criterion emphasises the active nature of the systems, requiring that the outputs can affect

369 (European Commission 2025d, 3). See also (Nessler and Wendehorst 2024, 12).
370 Similarly, also in (European Commission 2025d, 4). See also (Ebers 2024, 12; Nessler and Wendehorst 2024, 14).
371 (European Commission 2025d, 4).
372 AIA Recital 12.
373 In logic- and knowledge-based systems, inference could take place at the use phase, see (Nessler and Wendehorst 2024, 17).
374 In ML approaches, inference occurs in the development phase (Nessler and Wendehorst 2024, 17).
375 (European Commission 2025d, 5–6).
376 AIA Recital 12. See also (European Commission 2025d, 8; Hacker 2024a, 3).
377 AIA Recital 12 and (European Commission 2025d, 5–9).
378 AIA Recital 12 and (European Commission 2025d, 10–11).
379 (European Commission 2025d, 10).
380 (European Commission 2025d, 10).
381 (European Commission 2025d, 11).

physical or virtual environments, meaning the context in which the systems operate.[382]

As noted in prior research and discussed further in Chapter 5, simply classifying a system as an AI system does not automatically trigger many obligations, particularly for the deployers of such systems.[383] Instead, the majority of the specific technical and procedural requirements in the AIA apply only to high-risk AI systems. Under AIA Article 6(2) and Annex III, *high-risk AI systems* are those intended to be used for '*the recruitment and selection of natural persons, in particular, to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates*'.[384]

However, AIA Article 6(3) establishes a significant derogation[385] under which even systems intended for the aforementioned purposes would not be deemed high-risk systems and would therefore be exempt from the mandatory requirements imposed on high-risk AI systems.[386] Namely, under AIA Article 6(3), systems that do 'not pose a significant risk of harm to the health, safety or fundamental rights of natural persons', including by not materially influencing the decision-making outcome, would not qualify as high-risk AI systems. This could be the case only if the AI system fulfils one or more of the conditions listed in AIA Article 6(3).[387] The list includes situations where the AI system is intended to (a) perform a narrow procedural task[388], (b) improve the result of a previously completed human activity[389], (c) detect decision-making patterns or deviations from prior decision-making patterns and is not intended to replace or influence the previously completed human assessment, without proper human review,[390] or (d) perform a preparatory

382 AIA Recital 12 and (European Commission 2025d, 11–12).

383 See, e.g., (Bygrave and Schmidt 2024, 2; Hacker 2024c, 22).

384 AIA Annex III, point 4(a).

385 For instance, *Sandra Wachter* has deemed the derogations 'very vague and far reaching' (Wachter 2024, 685). For a more detailed analysis of this provision from a recruitment perspective, see (Publication IV / Parviainen 2026).

386 See also (Bygrave and Schmidt 2024, 5; Ebers 2024, 10).

387 It remains somewhat ambiguous how the provisions should be interpreted and what constitutes a significant risk. However, since it is a derogation from the main rule that aims to protect fundamental rights, it is to be interpreted narrowly (see, e.g., cases C-222/84 *Johnston*, para 36 and C-450/93 *Kalanke*, para 21). See also (Cristofolini 2024, 84; Leinarte 2024, 277).

388 Pursuant to Recital 53, these could be, for example, systems transforming unstructured data into structured data, systems classifying incoming documents into categories, or systems used to detect duplicates among a large number of applications.

389 As an example, Recital 53 mentions improving the language of already drafted documents.

390 Based on Recital 53, these could include checking humans' grading patterns to flag potential inconsistencies.

task to an assessment relevant for, among others, recruitment and selection purposes[391]. However, any system that profiles natural persons will always be classified as a high-risk AI system.[392] Pursuant to GDPR Article 4, point 4, profiling refers to automated processing of personal data to evaluate certain personal aspects relating to a natural person, especially analysing or predicting, among other aspects, that natural person's performance at work.[393] Section 2.4 below and Publication IV discuss in more detail the applicability of this exception in the recruitment context.

2.3 Algorithmic decision-making

A uniform definition of algorithmic[394] decision-making is absent in EU law. Instead, the various legislative instruments central to this dissertation adopt divergent, context-specific definitions, and none explicitly refers to the term 'algorithmic decision-making'.[395]

The GDPR regulates 'automated individual decision-making' which, according to Article 22(1), refers to 'a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.[396] In CJEU case law and prior research the key elements of automated decision-making have been divided into three as follows:[397] (i) a decision (whether final or intermediate) is made,[398] (ii) it is based solely on automated processing (i.e. without meaningful human involvement affecting the

391 Under Recital 53, the preparatory tasks could include, for instance, smart file-handling solutions such as indexing, searching, text and speech processing, and linking data to other data sources. Since these are only preparatory phases, their impact on the system's output should be very low.

392 AIA Art. 6(3).

393 See also (WP29 2018a, 7; Otto 2018, 395).

394 While the term 'algorithm' remains undefined in EU legislation, in computer science, it has been described, for instance, as a mathematical construct consisting of a chain of computational steps which transform an input into an output, see, e.g., (Cormen 2009, 5). *Davide Baldini and Matteo De Benedetto* have highlighted the open texture of the concept of algorithm, which, in the legal context, is further exacerbated by the open texture of legal discourse (Baldini and De Benedetto 2025, 1643–46).

395 Of varying scopes of algorithmic decision-making in different EU legislative instruments, see also (Rosin and Parviainen 2025, 481–85).

396 The requirement that the decision must be *solely* automated considerably limits the scope of automated decision-making (ADM). See (Publication II /Parviainen 2022, 235–36) and sections 4.2 and 5.2.1.2 below.

397 C-634/21 *Schufa*, para 43. Of scholarship preceding the Schufa judgement, see, e.g., (Publication II /Parviainen 2022, 236–37; Bygrave 2020, 532; Brkan 2019a, 99). For more recent scholarship, see, e.g., (Aza 2024, 11; Metikoš and Ausloos 2025, 217).

398 C-634/21 *Schufa*, judgment paras 44–46 and AG Pikamäe's Opinion para 43. See also (Aza 2024, 11; Metikoš and Ausloos 2025, 217–18).

outcome)[399], and (iii) it has legal or similarly significant effects on the data subject[400]. All of these elements must be met for a process to qualify as automated decision-making.[401] However, the CJEU confirmed in its *Schufa* judgment that these elements may be met within a multi-stage decision-making process, even when one organisation establishes a score and another makes a final decision based on it.[402] In this dissertation, decision-making described in GDPR Article 22(1) is referred to as automated decision-making (ADM).

In the AIA, two types of algorithmic decision-making are noted. First, AIA Article 86(1) mentions 'individual decision-making', which triggers a right to an explanation as 'a decision which is taken by the deployer on the basis of the output from a high-risk AI system'[403] and 'which produces legal effects or similarly significantly affects that person in a way which they consider to have an adverse impact on their health, safety or fundamental rights'.[404] This decision-making differs from the GDPR's ADM, as the AIA does not require the decision to be fully automated.[405]

Second, AIA also addresses a broader set of decision-making situations in Article 26(11). It requires that when high-risk AI systems 'make decisions or assist in making decisions related to natural persons' deployers of such systems (e.g., employers) must inform natural persons (e.g., job applicants) that they are subject to

399 C-634/21 *Schufa*, judgment paras 47 and 62 and AG Pikamäe's Opinion in paras 36, 43–47. See also (Aza 2024, 17; Palmiotto 2024, 216–17; Metikoš and Ausloos 2025, 218–22). The WP29 has also considered that to qualify as human involvement, the oversight of the decision must be meaningful, and not only 'a token gesture' (WP29 2018a, 21).

400 C-634/21 *Schufa*, para 48. See also (Aza 2024, 12–13; Metikoš and Ausloos 2025, 222–23; WP29 2018a, 21–22). GDPR Recital 71 mentions 'e-recruiting practices without any human intervention' as a potential situation where the decision has similarly significant effects.

401 C-634/21 *Schufa*, paras 43–50. See also (Aza 2024, 11), where it has been noted that the elements do not have to be fulfilled at the same time.

402 C-634/21 *Schufa*, paras 43–50. See also (Aza 2024, 13 and 16; Genicot 2025, 3–4). Of such multi-stage decision-making in scholarship prior to the Schufa judgement, see, e.g., (Binns and Veale 2021).

403 See AIA Recital 171. The wording of AIA Article 86(1) does not specify what 'on the basis of the output' means. That is, whether it must be the primary factor leading to the decision, whether a less significant influence on the decision could suffice, or whether fully automated decisions would fall within its scope. See also (Brkan and Palčič Vilfan 2024, 1203–4).

404 AIA Art. 86(1).

405 One interpretation is that fully automated decisions (such as ADM under the GDPR), are not covered by AIA Art. 86(1) at all, see also (Brkan and Palčič Vilfan 2024, 1203–4; Grozdanovski 2025, 15; Rosin and Parviainen 2025, 489). For discussion on the differences in the scope of GDPR Art. 22 and AIA Art. 86, see also (Publication IV / Parviainen 2026) and section 6.1.2.2 below.

the use of a high-risk AI system. The decision-making regulated in AIA Article 26 is not limited by the decision's effects[406] and applies more broadly to situations involving mere assistance in decision-making.

Similarly, prior scholarship has proposed varying definitions of algorithmic decision-making.[407] For example, *Dirk J. Brand* has succinctly defined algorithmic decision-making as 'decisions produced by algorithms or based on algorithms'.[408] In their study on algorithmic decision-making, *Claude Castelluccia* and *Daniel Le Métayer* have used the term 'algorithmic decision system' to refer to algorithms that support decision-making, analyse various data and involve different levels of human involvement ranging from semi-automatic to fully automated decisions.[409] Compared with legal definitions, the concepts presented in prior scholarship appear broader, encompassing algorithmic decision support regardless of system type.

In this dissertation, algorithmic decision-making is understood broadly and in a technology-neutral manner to include all situations in which algorithms[410] make decisions or assist in the decision-making process concerning individuals. Hence, algorithmic decision-making encompasses all legislated types of algorithmic decision-making relevant to the recruitment context (i.e., ADM, high-risk AI systems' decision-making and assistance in decision-making regardless of its effects), as well as other situations where algorithms support decision-making concerning job applicants. Nevertheless, as Chapter 5 will demonstrate, the legislated types of algorithmic decision-making are subject to the most comprehensive legal parameters and, therefore, receive greater attention in this dissertation than other types of algorithmic decision-making.[411]

2.4 Algorithmic recruitment system (ARS)

There is no statutory or judicial definition of algorithmic recruitment systems in EU law. This dissertation employs the term *algorithmic recruitment system* (ARS) as an

406 However, the definition concerns only high-risk AI systems, which are deemed to pose significant risks of harm to the health, safety or fundamental rights of natural persons (see AIA Art. 6).

407 See, e.g., (Brand 2020, 119; Breidbach 2024, 1). At times, the reader's familiarity with the concept is assumed, and no specific definition is provided, see, e.g., (de Laat 2022).

408 (Brand 2020, 119).

409 (Castellucia and Le Métayer 2019, 3–4).

410 See, e.g., (Cormen 2009, 5).

411 For instance, the use of a simple rule-based ARS to support human decision-making evades both the protections provided by the AIA and GDPR Art. 22. However, as will be shown in Chapter 5, it is still subject to certain more general restrictions and conditions.

umbrella term for a diverse range of machine-based and algorithm-driven systems utilised across various phases of the recruitment process to support human recruiters or automate certain parts of the process entirely.[412] ARSs may also assist with tasks other than decision-making, such as drafting job descriptions or job advertisements.[413] Beyond these shared features, ARSs differ considerably in terms of their tasks, complexity, capabilities, and degree of autonomy, among other factors.[414]

For clarity, I use the term ARS to refer collectively to all kinds of recruitment systems, without distinguishing among their specific characteristics or underlying technologies. Similarly, the term *algorithmic recruitment* refers to the general phenomenon of using ARSs. As will be shown in Chapter 5 below, the legal requirements set for ARSs vary depending on the technological approach and the level of human involvement. Thus, where a legal constraint or requirement applies exclusively to a particular category of systems (i.e., AI system, high-risk AI system, or ADM), I use the specific terms instead.[415] The remainder of this section briefly introduces the kinds of ARSs the term covers and whether those may fall within the more specific legal categories discussed above in sections 2.2 and 2.3.

A traditional and straightforward example of an ARS is a basic, transparent if-then algorithm, where the input is a job application and the output is feedback on whether the job application meets all predefined criteria. For example, *if* the applicant has a driver's license, *then* they proceed to the next phase of the recruitment process. *If* the applicant does not have a driver's license, *then* they do not proceed to the next phase. This type of ARS qualifies as algorithmic decision-making, as defined in section 2.3, because the algorithm at least supports recruitment decisions and, in some cases, can determine the outcome for certain applicants.

412 See also (Fabris et al. 2024, 3). The term 'automated hiring systems' is also used in prior literature, see (Sánchez-Monedero et al. 2020). Since the term 'automated' suggests that human recruiters are completely omitted, which is rarely the case, I prefer to use the term 'algorithmic recruitment'.

413 See section 3.1 below.

414 For a discussion on the differences between the ML-based and LLM-based systems, see section 3.3.4 below.

415 Although algorithms remain essential to these more recent recruitment systems, the algorithmic framing is less well-suited to describe LLM-based systems, and even less suitable for characterising the emerging agentic AI recruitment systems. There are many reasons for this unfitness. For instance, the traditional understanding of an algorithm may suggest rule-based, deterministic, and often explainable constructs, whereas LLMs are indeterminate, unpredictable, and non-interpretable. See sections 3.3 and 3.4 below.

Nevertheless, ARSs have long surpassed such basic automation. Many ARSs have been trained using machine learning (ML) techniques[416] to identify correlations between prior job applicants' characteristics and recruitment outcomes. These correlations are then used to predict the success of new job applicants.[417] However, state-of-the-art recruitment systems now exceed traditional ML-based systems in both complexity and capability.[418] Contemporary recruitment systems are increasingly built on LLMs, which provide a broader range of functionalities. For instance, such systems can allegedly evaluate job applicants' language proficiency or a particular skill based on unstructured data, such as their CVs, written responses, or video interviews.[419] Beyond LLM-based systems, emerging agentic AI recruitment systems represent a further development.[420]

The legal classification of varying ARSs turns first on whether they qualify as AI systems. Many state-of-the-art recruitment systems could satisfy the seven cumulative criteria of AIA Article 3, point 1[421] and thus be classified as AI systems.[422] First, such recruitment systems are computer-based, meaning that they fulfil the machine-based criterion.[423] Second, considering the aims pursued with recruitment systems, these systems are typically designed to perform certain operations, such as screening CVs, with some degree of autonomy.[424] Third, since adaptiveness is an optional criterion under the definition, the fact that recruitment systems often are non-adaptive[425] does not place them outside the scope of AI systems. Fourth, the criterion of operating towards explicit or implicit objectives would also be satisfied by recruitment systems. For instance, an explicit objective for a system that drafts job advertisements could be to optimise the language used to ensure inclusivity. Through training data, such a system could learn an implicit

416 The aim of machine learning is to create computer systems that improve automatically through experience, using methods such as supervised learning, unsupervised learning and reinforcement learning (Jordan and Mitchell 2015).

417 (Kelly-Lyth 2021, 902–3; Sánchez-Monedero et al. 2020; Kleinberg et al. 2018, 134–37)

418 For practical use cases, see section 3.1 below.

419 See, e.g., (Gan et al. 2024). For more practical use cases of LLMs in recruitment, see (Heymans 2024). For a more detailed explanation of LLM-based recruitment systems, see section 3.3.2 below.

420 See section 3.3.3 below.

421 See section 2.2 above.

422 (Publication IV / Parviainen 2026). This applies both to traditional ML-based ARS and LLMs.

423 See AIA Recital 12 and (European Commission 2025d, 2–3). Similarly, also (Voigt and Hullen 2024, 5).

424 Of the pursued benefits of the ARSs, see, e.g., (Horodyski 2023, 7).

425 See, e.g., (Kelly-Lyth 2021, 927). However, for instance, targeted advertisements might use also some dynamic algorithms (Bogen and Rieke 2018, 44).

objective of avoiding certain types of language. The fifth criterion of inference could be the most limiting factor, as it may exclude some recruitment systems from the definition of an AI system.[426] Nevertheless, recruitment systems powered by ML or LLMs would likely satisfy the inference criterion.[427] Finally, the sixth and seventh criteria are often met, since the outputs produced by recruitment systems, such as scores for CVs or interviews, typically fall within the output categories of predictions, content, recommendations, and decisions, and are specifically generated to influence the recruitment process. Nevertheless, not all recruitment systems necessarily fulfil the criteria for AI systems, for instance, because simple software systems lack the capability to infer.[428] Consequently, the applicability of the AI system definition must be assessed separately for each ARS.[429]

ARSs that qualify as AI systems frequently, but not invariably, fall within the scope of high-risk AI systems under the AIA.[430] ARSs are intended to be used in the high-risk use case of the recruitment and selection of natural persons.[431] Further, many AI-based recruitment systems process job applicants' personal data to evaluate or predict aspects related to job applicants, such as potential work performance, which constitutes profiling under GDPR Article 4, point 4,[432] thereby rendering the derogation in AIA Article 6(3) inapplicable.[433] However, not all AI-based recruitment systems necessarily profile job applicants.[434] When determining whether a given ARS engages in profiling, and thus whether it falls outside the AIA Article 6(3) derogation and retains its classification as a high-risk AI system, the Article 29 Working Party (WP29) guidance on profiling offers a persuasive interpretative reference point. According to the WP29, the essential elements of profiling under the GDPR include that (i) it is an *automated* form of processing, (ii) which is carried out on *personal data*, and (iii) it has the objective to *evaluate personal aspects* about

426 AIA Recital 12 highlights the importance of this criterion. Similarly (European Commission 2025d, 5).

427 AIA Recital 12 and (European Commission 2025d, 6–7).

428 (European Commission 2025d, 8). For instance, the simplest if-then algorithms, or even more complex ARSs that rely directly on human-defined rules, would not include all the required elements, since they do not infer how to decide their outputs. See also (Hermanns et al. 2024, 4–5).

429 (European Commission 2025d, 1).

430 (Publication IV / Parviainen 2026).

431 AIA Annex III, point 4(a).

432 See also (WP29 2018a, 7; Otto 2018, 395).

433 See section 2.2 above.

434 In general, it has been assumed that the exemption could be important in practice, allowing providers to avoid obligations and costs related to high-risk AI systems (Bird & Bird 2024, 6).

a natural person.[435] Some systems may simply process applicant data without performing any evaluative function or may process non-personal data. For example, an AI system might transfer data from one system (e.g., email) to another (e.g., a recruitment platform). Such processing could be categorised as a narrow procedural[436] or preparatory task[437], possibly allowing the AI system to be classified as a non-high-risk under AIA Article 6(3).[438]

With regard to ADM, many ARSs could make decisions as broadly interpreted by the CJEU[439] and some of those decisions can have legal effects or at least similarly significant effects on the job applicants.[440] However, the decision may not be solely automated if a human is meaningfully involved in the decision-making process.[441] An ARS may perform different functions across the various stages of the recruitment process, encompassing varying degrees of human involvement. Even when a human makes the final selection decision, earlier stages of the process, such as targeted job advertising and CV screening, could be entirely automated.[442] Thus, for certain applicants, the recruitment process may have factually ended during these earlier stages, for instance, if they are not shown the job advertisement or are screened out as unsuitable for the position.[443] Consequently, when an ARS conducts or assists with multiple tasks in the recruitment process, it is crucial to assess separately for each task

435 (WP29 2018a, 6–7). The WP29 has stated that the word 'evaluating' implies that some form of assessment or judgment about a person is made. Hence, the basic classification of individuals based on known characteristics does not necessarily constitute profiling.

436 AIA Art. 6(3)(a).

437 AIA Art. 6(3)(d).

438 See also (Publication IV / Parviainen 2026).

439 C-634/21 *Schufa*, paras 44–46. The CJEU has emphasised the broad scope of the concept 'decision' and, based on GDPR Recital 71, highlighted that it may include a measure, such as e-recruiting practices without human intervention. See also (Publication II /Parviainen 2022, 234–35).

440 According to the WP29, legal effects affect someone's legal rights, legal status or their rights under a contract. As regards similarly significant effects, the WP29 has specifically mentioned 'decisions that deny someone an employment opportunity or put them at a serious disadvantage' as ones being sufficiently significant to meet the GDPR Article 22(1) threshold. For more precise criteria for analysing significance, see (WP29 2018a, 21–22). See also C-634/21 *Schufa*, paras 48–49 and (Publication II /Parviainen 2022, 236–37).

441 The WP29 has highlighted that token gestures and the routine application of automatically generated profiles do not constitute meaningful human involvement. It has required that the person involved in the process should have 'the authority and competence to change the decision' and they 'should consider all the relevant data' (WP29 2018a, 20–21).

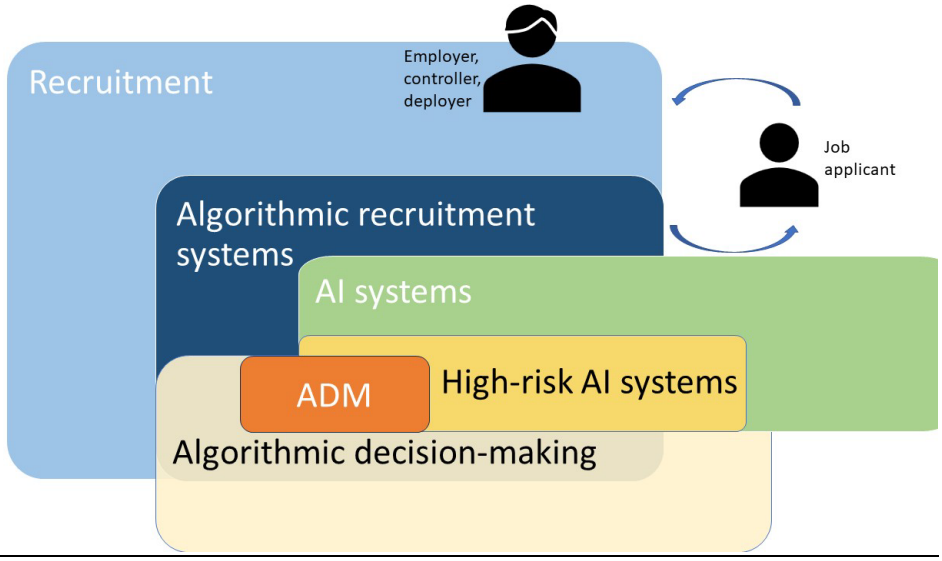
442 In *Schufa*, the creation of the profile was automated, and as the bank drew strongly from the profile when granting loans, the decision was solely automated, C-634/21 *Schufa* paras 47–48. See also (Bogen and Rieke 2018, 26; De Stefano and Wouters 2022, 11; Gavaghan et al. 2021, 47).

443 (Reynolds and Dickter 2017, 856; Bogen and Rieke 2018, 26; Parodi 2024, 122).

whether the criteria for ADM under GDPR Article 22 are met.[444] Since at least some stages of the recruitment process typically involve meaningful human involvement (e.g., making the final selection from a shortlist of a few candidates), ADM is less likely to be applicable if the recruitment process is assessed only in its entirety.[445]

ADM and AI systems are also often interlinked. ADM could be part of an AI system, or it could also occur in other types of ARSs, such as systems operating based on purely human-defined rules. Not all AI systems make automated decisions either. However, when an ARS is an AI system and conducts ADM, it qualifies as a high-risk AI system.[446] The intricate relationships between the different concepts are depicted in Figure 1. The potential use cases, lifecycle and technologies behind the ARSs will be discussed in more detail in Chapter 3.

Figure 1: Key concepts



444 In the *Schufa* judgment (C-634/21), the CJEU emphasised many times the context-specificity of the interpretation (see, e.g., paras 49, 50, 61 and 62).

445 The broad concept of the decision upheld in the *Schufa* judgment (C-634/21, paras 44–46) hints that it is not only the final decisions, but also the intermediate ones, which could be automated. Nevertheless, it remains to be seen how GDPR Art. 22 is applied in the recruitment context.

446 See AIA Art. 6(3), which mentions that significant risks would not occur if there is no material influence on the decision-making. In ADM, there will always be a material influence on decisions, and these decisions have legal or similarly significant effects, often significantly affecting the job applicants' fundamental rights. See also (Palmiotto 2024, 220–21).

Figure 1 also includes the parties central to the use of ARSs: employers as users of ARSs in their varying statutory roles, and job applicants. The following sections will explain what this dissertation means when referring to these actors.

2.5 Employer: controller, deployer

Varying terms are used in relevant EU legislation to refer to the entity using an ARS. In the context of EU labour law, entities that use ARSs are typically employers.[447] However, in certain situations, ARSs may also be utilised by recruitment agencies or other entities within a company group to which the employer has outsourced recruitment tasks.[448] Nevertheless, in this dissertation, the analysis is made based on the assumption that employers are the parties using ARSs. With the term employer I refer to the entity with which the job applicant, if chosen, would enter into an employment contract.[449] For the purposes of this dissertation, it is not necessary to examine in detail the challenges that may arise in defining the correct employer(s).[450]

Under the GDPR, the employer using the ARS will generally act as a controller and be primarily responsible for compliance with the data protection legislation.[451] Pursuant to Article 4, point 7 of the GDPR, the controller is the entity which, alone or jointly with others, determines the purposes and means of processing personal data. EDPB guidelines clarify that determining requires exerting decisive influence on the purposes ('why') and means ('how') of processing.[452] The EDPB has

447 In EU labour law, much less attention has been given to defining the concept of an employer than to that of an employee. See, e.g., (van Schadewijk 2021, 363; Deakin 2001, 72). Yet, the concept of the employer has also been examined closely, see e.g., (Prassl 2015).

448 In such a case, this other entity using an ARS should also consider the legal parameters discussed in Chapter 5. Yet, depending on the situation, the other entity might also be a processor under GDPR Art. 4, point 8, which could affect its GDPR-based responsibilities.

449 See also (van Schadewijk 2021, 363–64; Deakin 2001, 73; Countouris and De Stefano 2019, 62–63).

450 In traditional employment settings, identifying the employer using the above-mentioned contract-based definition may be rather straightforward (van Schadewijk 2021, 363–64; Deakin 2001, 73; Countouris and De Stefano 2019, 62–63). Yet, under certain circumstances, the contract-based definition is too simplistic, and a functional approach, considering the facts of the case, is required instead (see case C-610/18 *AFMB Ltd and Others v Raad van bestuur van de Sociale verzekeringsbank*, paras 38 and 56–61). For instance, if the recruitment process is outsourced to a parent company which also exercises authority over the recruited person when work is performed, questions regarding the correct employer entity may arise.

451 GDPR Arts. 5(2) and 24. See also (EDPB 2021, 7).

452 (EDPB 2021, 13–14). Of the criteria of decisive influence, see also case C-40/17 *Fashion ID*, para 78.

considered that the employer processing personal data about its employees will generally be the one who determines the purposes and means of processing and thus acts as a controller.[453] Typically, this also applies when using an ARS,[454] as the employer decides that personal data is processed to conduct certain recruitment activities using the ARS.[455]

Under the GDPR, the allocation of controller and processor roles in algorithmic recruitment can be complex. Outsourcing the recruitment process to a recruitment agency does not, in itself, alter the employer's status as a controller. Where the recruitment agency processes personal data solely on the employer's behalf and in accordance with its instructions to provide recruitment services, the agency acts as a processor under GDPR Article 4, point 8.[456] However, joint controllership under GDPR Article 26 may arise where the recruitment agency pursues its own purposes in processing and, together with the employer, decides on the purposes and means of processing,[457] as illustrated by the EDPB guidelines' example concerning combined CV databases.[458] Similarly, where an ARS provider exercises decisive

453 (EDPB 2021, 12).

454 See also (EDPB 2021, 12; Barberá 2025, 43).

455 See also (EDPB 2021, 13), where there is an example of standardised cloud storage services. Using an ARSs to process job applicants' personal data could be a rather similar situation.

456 See also (EDPB 2021, 21). An interesting question is also whether the recruitment agency may independently decide to utilise an ARS. The EDPB has emphasised that the essential means, such as the type of personal data, duration of processing and categories of data subjects, should always be decided by the controller. However, the EDPB has considered that the choice of software is a non-essential matter that remains within the processor's authority (EDPB 2021, 15). Particularly where the ARS conducts ADM, it could be deemed as an essential matter which the processor could not unilaterally decide. For clarity, it could be helpful to include a clause on the use of ARS in data processing agreements between employers and processors.

457 Drawing the line between processors and joint controllers could be tricky in practice. Of the criteria in deciding joint-controllership, see (EDPB 2021, 18–25) and cases C-210/16 *Wirtschaftsakademie*, paras 34–40, C-25/17 *Jehovan todistajat*, paras 71–75 and C-40/17 *Fashion ID*, paras 74–80. The GDPR-based legal parameters discussed in Chapter 5 should be noted by both joint controllers.

458 (EDPB 2021, 23). The EDPB's example is roughly as follows. In a situation where a recruitment agency seeks potential applicants from both CVs provided by the employer and from its own CV database, the agency and employer participate in the processing with the purpose of finding suitable applicants. The converging decisions, then, are the recruitment agency's decisions to create and manage the recruitment service, including the CV database, and the employer's decision to enrich the agency's database with the CVs that applicants have directly sent to it. Since these decisions complement each other and are necessary for finding suitable applicants for the employer, the recruitment agency and the employer would be joint controllers for this particular processing operation.

influence over the purposes and means of processing, it may qualify as a joint controller rather than as a mere processor, or not even that.[459] Especially if the ARS is provided as a service, the possibility of the provider's joint controllership exists.[460] However, a detailed analysis of these scenarios falls outside the scope of this dissertation. For present purposes, it is assumed that the employer acts as the sole controller during the use phase.

Employers using ARSs seldom develop the systems in-house and instead purchase them from specialised providers.[461] Based on AIA Article 3, point 4, employer organisations that decide to utilise AI-based ARSs under their own authority are typically categorised as *deployers*.[462] In contrast, AIA Article 3, point 3, defines *providers* as persons or bodies that develop an AI system or a GPAI model, or have one developed, and place it on the market or put it into service under their own name or trademark. However, drawing the line between providers and deployers is not always that simple.[463] Employers may also become providers if they substantially modify an existing high-risk AI recruitment system[464] or repurpose an AI or GPAI system that has not been classified as high-risk, so that it becomes a high-risk AI system due to its new purpose (e.g., use in CV screening).[465] For example, using ChatGPT to screen job applications could be a scenario in which an employer is assigned the responsibilities of both providers and deployers under the

459 In any case, for the processing of personal data in the development phase, the provider typically is the controller.

460 *Michele Molé* has argued that actually the providers of algorithmic management services often decide the data collected, the ways of evaluation, and decision-making criteria (Molè 2025, 174). Of the providers' joint-controllership in general, see also (Hacker 2024c, 22–23; Cobbe and Singh 2021, 22–31).

461 (ICO 2023, 74; Bogen and Rieke 2018, 14; Cristofolini 2024, 86; Yusifli 2024, 229).

462 See also (Feiler and König 2024, 61; Barberá 2025, 43). The employer organisation would then be the deployer, not the individual recruiter utilising the AI-based ARS (Voigt and Hullen 2024, 14).

463 Difficulties could arise, for instance, if the employer utilises a Software as a Service (SaaS)-based system, creating their own ARS by combining various elements offered by the provider (Voigt and Hullen 2024, 14–15). Of the AI as a service model, see also (Cobbe and Singh 2021).

464 See AIA Art. 25(1)(b). According to AIA Art. 3, point 23, substantial modification is 'a change to an AI system […] which is not foreseen or planned in the initial conformity assessment […] and as a result of which compliance of the AI system with requirements set out in Chapter III, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed'. AIA Recital 128 mentions change of operating system or software architecture as potentially giving rise to substantial modifications.

465 See AIA Art. 25(1)(c). Another situation where employers could become providers includes putting their name or trademark on a high-risk AI system that has been placed on the market or put into service (AIA Art. 25(1)(a)).

AIA.[466] Particularly where the AI system was not originally considered a high-risk system, compliance with the provider obligations is likely to be exceptionally burdensome.[467] Nevertheless, the initial provider should cooperate closely and provide the information and assistance required if it has not clearly specified that the AI system may not be modified into a high-risk system.[468]

The allocation of responsibilities differs across the relevant legal instruments. Under the AIA, the majority of the requirements fall on providers, although deployers also face significant duties.[469] Instead, under the GDPR, most obligations rest on controllers, i.e., the deployers when AI systems are used.[470]

This dissertation uses the term *employer* to refer generally to the entity that uses an ARS, which is treated as the controller under the GDPR and the deployer under the AIA. As mentioned, this is a simplifying assumption. Where differentiation between various statutory roles is analytically necessary, this dissertation uses the specific terms, controller or deployer.[471] The term *ARS provider* refers to the entity that develops and places an ARS on the market.[472]

2.6 Job applicant

EU law contains no statutory or judicial definition of the term *job applicant*. Therefore, this dissertation establishes a working definition. Since ARSs can affect individuals at stages that precede or bypass formal application procedures entirely,

466 For example, OpenAI's Usage policy updated 29 January 2025 states: 'Don't perform or facilitate the following activities that may significantly impair the safety, wellbeing, or rights of others, including: […] 2. Making high-stakes automated decisions in domains that affect an individual's safety, rights or well-being (e.g., […] employment .[…])', see (OpenAI 2025b). Hence, those appear to prevent automated decision-making, but not other potentially high-risk AI use cases.

467 See also (Riede and Talhoff 2024, 532–33). The provider obligations presuppose access to detailed technical information about the system's design and training data, among others, which an employer repurposing a third-party system will typically lack.

468 AIA Art. 25(2). See also (Riede and Talhoff 2024, 533).

469 For instance, the majority of the requirements set for high-risk AI systems and obligations related to those set in AIA Chapter III concern the providers. Of the deployer's obligations, see AIA Arts. 4, 5 and 26 as well as Chapter 5 below. AIA Recital 91 states that AI systems' nature and risks to safety and fundamental rights that their use may cause, as well as the need to ensure proper monitoring of the AI system's performance in real-life settings, require duties to be set for deployers as well.

470 (Hacker 2024c, 22–23; Cobbe and Singh 2021, 21). During the development phase, the provider typically serves as the controller for the processing of personal data.

471 The authorities' guidance and CJEU case law also use the terms controller or deployer.

472 This party would be a provider under AIA Art. 3, point 3, and, depending on its participation in the processing of personal data, either a joint-controller, a processor, or none of those under the GDPR.

defining job applicants narrowly by reference to formal participation alone would exclude persons most exposed to certain ARS-related risks. Hence, a broader effects-based definition is necessary.

This broader definition is primarily derived from the CJEU case law concerning the Non-Discrimination Directives in the recruitment context. In several cases involving public statements about discriminatory recruitment practices, the CJEU has held that there does not have to be an identifiable victim, provided that the measure could affect certain job applicants' access to the labour market.[473] This reasoning supports an approach in which job applicant status is determined not by participation in a formal recruitment procedure but by exposure to the effects of a recruitment practice.

Accordingly, for the purposes of this dissertation, a job applicant refers to any person whose employment opportunities are affected by specific recruitment practices, regardless of whether they have formally applied for any position. The practical scope of this definition can be illustrated along a spectrum. At its core are persons who have actively applied for an open position or submitted an open application.[474] These situations are mostly addressed in this dissertation. At the outer boundaries of the definition are persons who have not taken any active steps to apply for a job but nonetheless have been affected by an ARS. For instance, where the employer uses an ARS to distribute job advertisements to a defined audience, individuals excluded from that audience on the basis of a protected characteristic could be adversely affected and potentially discriminated against without ever becoming aware of an open position.[475] Nevertheless, as such practices have affected these individuals' employment opportunities, this dissertation regards them as job applicants.

It must be noted that this dissertation's definition of a job applicant is not fully aligned with the personal scope of the GDPR. The GDPR applies only to the processing of personal data, and job applicants whose personal data is processed in an ARS qualify as *data subjects* under the GDPR.[476] The legal safeguards stemming from the GDPR apply on this basis.[477] However, ARS-related harm can arise without any processing of the affected individual's personal data, for instance, where an

473 See e.g, cases C-54/07 *Feryn*, para 25, C-81/12 *Asociata Accept*, para 52, C-507/18 *Associazione Avvocatura per i diritti LGBTI,* paras 39–43.

474 However, in case *Kratzer* (C-423/15, paras 29 and 34–35), the CJEU considered that although the EED and GED protect persons seeking employment, the protection did not apply if the applicant's sole purpose was to obtain a formal applicant status in order to claim compensation under the directives.

475 (Parodi 2024, 112).

476 GDPR Arts. 2 and 4 point 1.

477 See section 6.1 below for a more detailed discussion on the safeguards.

employer's use of an ARS prevents a disabled individual from submitting an application.[478] Although the GDPR is inapplicable[479] in such cases, the Employment Equality Directive (EED) could already be triggered.

Having established these foundational concepts, the analysis can now turn to the systems at the heart of this dissertation. The following chapter examines the practical functions of ARSs, outlines their typical lifecycle, traces recent technical developments, and discusses their founding characteristics.

[478] Such individuals are considered job applicants within the meaning adopted in this dissertation, as their employment opportunities are adversely affected.

[479] Although no personal data of that particular job applicant would be processed, the employer's obligations as a controller under the GDPR would require it, nevertheless, to inform about the processing of personal data in the recruitment process. See GDPR Art. 13 and section 5.2.2 and 6.1.2.1 below.

3 AI and Algorithmic Recruitment – Evolution and Key Characteristics

3.1 Use cases in contemporary recruitment

ARSs can assist in various stages of the recruitment process, and new solutions are frequently launched.[480] This subchapter provides a general overview of potential ARS use cases and the related issues discussed in prior scholarship.

To begin with, ARSs can aid in *sourcing* job applicants, for instance, by drafting job descriptions[481] and advertisements[482] as well as optimising their visibility and delivery.[483] Search, ranking, and recommendation algorithms play a critical role in determining which job openings applicants see and which applicants come to recruiters' attention.[484] The sourcing ARSs could facilitate the identification of highly specialised passive candidates[485] for niche roles. For positions that attract a high volume of applicants, recommendation algorithms and targeted advertising help identify applicants who are most likely to be suitable for the role. Although

480 (Bogen and Rieke 2018, 14). For recent unofficial statistics on the AI recruitment market, see (Kumar 2025).

481 (Walker and Larson 2025; Bogen and Rieke 2018, 15). Many generative AI solutions could assist with drafting job descriptions, and there are also numerous tools specifically designed for that task, see e.g., (Joveo 2025; Gohire.io 2025; Job Description.ai 2023).

482 (Black and van Esch 2020, 219; Chen 2023, 139). While general generative AI applications could be useful in this regard, there are also targeted solutions to specifically address the risk of biased job advertisements, see, e.g., (Textio 2023; Witty.works 2025; Gender Decoder 2025).

483 (Fabris et al. 2024, 3; Bogen and Rieke 2018, 14 and 17; Parodi 2024). For an example solution for targeting and campaigns, see e.g., (Jobilla 2025).

484 (Fabris et al. 2024, 3; Chala et al. 2018; Alexander III et al. 2025, 3). These kinds of algorithms are used, for instance, in social networks such as LinkedIn, see, e.g., (Agarwal 2018).

485 Suen defines passive candidates as persons who are not actively searching for a new job, but who could be willing to change jobs if a good opportunity arises. Passive candidates are assumed to be more competent and have better employment records, but are more difficult to solicit than candidates actively searching for new work (Suen 2018, 397).

algorithmic sourcing tools could benefit both recruiters and job applicants by improving the efficiency, accuracy, and scalability of sourcing, these tools may also affect the diversity of the applicant pool.[486] For instance, the targeting and delivery of job advertisements could exclude certain applicant groups, limit their access to work, and discriminate against them.[487]

ARSs have considerable potential also in the *screening* phase.[488] Instead of screening applications and CVs for preset keywords (e.g., degrees or experience)[489], ARSs can also identify synonyms and infer equivalent capabilities from natural language.[490] Furthermore, ARSs could diversify the screening methods. There are, for example, games to measure soft skills or conduct psychometric assessments,[491] questionnaires to assess personality or job performance[492] as well as chatbots to query questions that assist in filtering and prioritising candidates.[493] When the number of applications is high, the majority of applicants could be rejected in the screening phase without (or with only nominal) human discretion.[494] ARSs used in the screening phase could raise concerns about data protection, such as data minimisation, accuracy, profiling, and automated decision-making, as well as non-discrimination, if screeners exhibit bias against certain applicant groups.

486 (Bogen and Rieke 2018, 18; Kim and Scott 2018, 114; Parodi 2024, 111; Alexander III et al. 2025, 3). For instance, the wording of the job description could affect the diversity of the applicant pool, see e.g. (Gaucher et al. 2011).

487 (Parodi 2024; Imana et al. 2021; Bogen and Rieke 2018, 18; Kim and Scott 2018, 114; Dalenberg 2018). *Anja Lambrecht and Catherine Tucker* have shown that even gender-neutral ads have been displayed more to men than women (Lambrecht and Tucker 2019). Similar practices appear to continue, as the Netherlands Institute for Human Rights recently found that Meta indirectly discriminated on the basis of gender when determining which job advertisements were shown on Facebook (ANP 2025).

488 (Fabris et al. 2024, 4; Chen 2023, 140–41; Black and van Esch 2020, 220; Sivathanu and Pillai 2019, 459; Cohen 2019, 63; Bogen and Rieke 2018, 26). For available solutions assisting in applicant screening, see e.g., (Oleeo 2025; CVViz 2023; Zoho Recruit 2025).

489 (Bogen and Rieke 2018, 26; Gavaghan et al. 2021, 13–14)

490 (Black and van Esch 2020, 220; Hunkenschroer and Luetge 2022, 991–93).

491 (Fabris et al. 2024, 4; Sánchez-Monedero et al. 2020; Lievens and Chapman 2019, 139; Bogen and Rieke 2018, 32–34; Bodie et al. 2017, 973–75; Chamorro-Premuzic et al. 2016, 631–32; Arthur et al. 2017, 971–75; Peck 2013). For practical examples of gamification, see e.g., (pymetrics 2023; HireVue 2023; Artic Shores 2025).

492 (Fabris et al. 2024, 4; Bogen and Rieke 2018, 30). See, e.g., (Sapia.ai 2025).

493 (Fabris et al. 2024, 4; Bogen and Rieke 2018, 26–28; Sivathanu and Pillai 2019, 459; Chandler 2017). See, e.g., (Jotform 2025; Humanly 2025).

494 (Bogen and Rieke 2018, 26; Centre for Data Ethics and Innovation 2021, 47).

Although *interviewing* is typically the stage in which recruiters directly communicate with applicants,[495] several ARSs have been developed to assist in this stage to save time and to standardise interviews.[496] For example, chatbots could interview candidates over the phone or via video link.[497] Additionally, ARSs can assist in evaluating interviews conducted by humans, such as assessing applicants' responses, expressions, and tone of voice.[498] Video interviewing has also raised multiple concerns, ranging from automated processing of unnecessary personal data (e.g., skin colour) and accuracy[499] to discrimination based on disability or ethnicity.[500]

While human recruiters still often make the final recruitment decisions on whom to hire,[501] there are specific tasks in the *selection* stage that might, nevertheless, be assisted by ARSs. The employer might, for instance, require some background checks to be conducted before the employment contract is signed.[502] Algorithmic social media background checks[503] and automated reference checks[504] might be used at this point. However, such checks could be problematic from both the perspective of data protection and non-discrimination.[505] Furthermore, when negotiating employment terms, ARSs can help predict the salary and additional benefits that applicants are willing to accept.[506] These systems could also raise the risk of

495 (Bogen and Rieke 2018, 36). On the importance of interviews as part of the recruitment process, see, e.g. (Macan 2009, 203; Levashina et al. 2014, 241–42).

496 (Bogen and Rieke 2018, 36; Langer et al. 2019, 302; Gikopoulos 2019, 59; Hunkenschroer and Kriebitz 2023, 200; Reynolds and Dickter 2017, 860). See, e.g., (JOBMA 2025; HireVue 2023), which offer one-way video interviews.

497 (Gavaghan et al. 2021, 14). See, e.g., (Humanly 2025).

498 (Bogen and Rieke 2018, 36–38; Gavaghan et al. 2021, 14). For instance, Hirevue assists in analysing the video interviews (HireVue 2023). There are also AI assistants that automatically generate notes of the interviews, allowing human recruiters to focus on the conversation, see e.g., (Metaview 2025).

499 (Bogen and Rieke 2018, 37; Kammerer 2021; Tippins et al. 2021).

500 (Kammerer 2021, 828–31; Bogen and Rieke 2018, 38; Köchling and Wehner 2020). Discrimination on multiple other grounds could also emerge. Furthermore, certain applicants may be disadvantaged due to inadequate access to technology or a lack of digital skills.

501 (ICO 2024, 32; Carter 2024, 351–52; Bogen and Rieke 2018, 39).

502 (Albert 2019, 217; Bogen and Rieke 2018, 39).

503 (Kong and Ding 2024, 35, 49–50; Bogen and Rieke 2018, 39–40; WP29 2017b, 11). There are several vendors for social media background checks, see e.g., (Ferretly 2025; Hireright 2025).

504 ARSs could run scans on different databases to authenticate references (Sen et al. 2023, 2). There are varying solutions on the market. For example, SociaFinder.ai claims to find anyone online with a picture, in order to verify whether they are who they claim to be (SocialFinder.ai 2025).

505 (Kong and Ding 2024, 35, 49–50; Bogen and Rieke 2018, 39–40; WP29 2017b, 11).

506 (Fabris et al. 2024, 4; Bogen and Rieke 2018, 39 and 41; Meng et al. 2022).

discrimination, for instance, if women or people of colour are more likely to accept lower salaries due to prior societal imbalances, which the system then reinforces.[507]

The use cases discussed above illustrate what the ARSs are capable of in practice once deployed. However, ARSs undergo several phases before they reach operational use. The following subchapter outlines the typical lifecycle of ARSs.

3.2 Algorithmic recruitment systems' lifecycle

Although this dissertation focuses on the constraints that apply during the use phase of ARSs, a general understanding of the entire lifecycle remains necessary, as decisions made in earlier stages may impact ARSs and their users' compliance with EU legislation.[508] A basic example is the use of protected grounds, such as gender or race, or their inextricably linked proxies[509] as decision-making criteria during the design and training phases, which may eventually render the system discriminatory. Knowledge of the lifecycle also clarifies the roles and responsibilities of the actors involved in developing and using ARSs.

Given the limited research on the lifecycle of ARSs specifically, this discussion draws on definitions and scholarship on the lifecycle of AI and algorithmic systems more broadly. However, there is currently no statutory or judicial definition of the lifecycle of an algorithmic or AI system, despite repeated references to it in the AIA.[510] Prior research offers no unanimous definition either. In prior computer science research, the lifecycle is often divided into design, development and deployment.[511] The OECD provides a widely cited definition of the AI system lifecycle, comprising the following: i) plan and design; ii) collect and process data; iii) build model(s) and/or adapt existing model(s) to specific tasks; iv) test, evaluate, verify and validate; v) make available for use/deploy; vi) operate and monitor; and vii) retire/decommission.[512] In some OECD materials, the lifecycle

507 (Bogen and Rieke 2018, 41–42).

508 From the perspective of non-discrimination, see e.g., (Barocas and Selbst 2016) and from the perspective of data protection, see (EDPB 2024b, 4).

509 Proxies refer to neutral features that correlate with protected grounds. For a more in-depth analysis of the inextricably linked proxies, see (Publication III / Parviainen 2024).

510 AIA Arts. 9, 15 and 40, Annex IV Section 6, as well as Recitals 65, 69, 73 and 75 refer to high-risk AI system's lifecycle. In addition, AIA Recitals 110, 114 and 115 target the general-purpose AI model's lifecycle.

511 See, e.g. (Silva and Alahakoon 2022, 4; Desouza et al. 2020). However, the terms used for these stages vary. For example, *Marabelli et al.* have used the tripartition of *design – implement – deploy,* see (Marabelli et al. 2021, 2), and *Laato et al.* have referred to *design – development – operation* trisection, see (Laato et al. 2022, 113). For detailed divisions covering more stages, see, e.g. (Schearer 2000; Amershi et al. 2019, 292).

512 (OECD 2024, 8).

has been simplified to include only four stages.[513] To support the subsequent legal analysis, the following section presents a simplified lifecycle of an AI recruitment system that relies on ML, following the OECD's more concise picture of the AI system lifecycle.[514] However, when the ARS is not ML-based, or if it is built on a GPAI model[515], some of the stages described below may not apply in full.

In AI recruitment systems built solely for that purpose, *the design, data, and models phase* is the first stage of the project, which comprises 'planning and design, data collection and processing, as well as model building'.[516] The lifecycle begins with defining the problem the system aims to solve and setting clear objectives for the system, such as improving hiring efficiency or reducing bias in recruitment decision-making.[517] Thereafter, several critical data-related steps follow, including data collection, procurement, preparation, labelling, and exploration.[518] Further, the system architecture is designed, and the models and algorithms are chosen[519] considering factors such as transparency[520] and technical integration with the existing HR infrastructure.[521]

Once the models and their basic parameters are defined, training begins. Training involves running a computer program to optimise the model's parameters using methods with varying levels of human input, such as supervised[522], semi-

513 These include i) design, data and models; ii) verification and validation; iii) deployment; and iv) operation and monitoring (OECD 2025).

514 The EDPB has also chosen to streamline the stages of the AI lifecycle in its Opinion 28/2024, in which it used only the development and deployment phases; see (EDPB 2024b, 11).

515 See section 3.3.2 below for more details of these.

516 (OECD 2025).

517 (Silva and Alahakoon 2022, 4–5; Passi and Barocas 2019).

518 (Silva and Alahakoon 2022, 4–5; Amershi et al. 2019, 292–93). The AIA Art. 10 sets notable requirements on data and data governance.

519 (Silva and Alahakoon 2022, 4, 6–7; ICO 2023, 120). The models and algorithms may range from proprietary machine learning models to large language models fine-tuned for recruitment tasks. For instance, the AI recruitment system's provider might use GPT-4 as a base model and fine-tune it for recruitment tasks, such as resume screening and candidate ranking, see, e.g., (Ohm 2024).

520 Some models are inherently unexplainable, see, e.g., (ICO 2023, 120).

521 AI recruitment systems can be integrated into existing HR systems, deployed as standalone software or hosted as cloud-based services. See (Jones 2024).

522 In supervised learning, the developers provide the algorithm with correct input-output pairs, and based on these examples, the algorithm is expected to learn how to perform on unseen inputs (Alpaydin 2020, 11).

supervised,[523] unsupervised[524] or reinforcement learning[525]. Regardless of the chosen training method, the goal is to optimise the model's performance by iteratively adjusting (i.e. tuning) the parameters using the data or past experience.[526] Throughout training, the model is validated against chosen performance metrics and parameters are adjusted accordingly to meet the predefined targets.[527] Decisions made during the design, data, and models phase of an AI recruitment system's lifecycle can already significantly impact compliance with data protection and non-discrimination legislation.[528]

With the recruitment systems based on GPAI models, the first stage of the lifecycle diverges from traditional ML systems. For GPAI-based recruitment systems, the design stage could comprise, among other elements, decisions on which GPAI model to adopt, the scope of the recruitment tasks to be delegated, and the adaptation strategy. Adaptation may involve fine-tuning, in-context learning and/or the introduction of specific quardrails to align the model with recruitment objectives.[529] Since these systems rely on pretrained models, the role of data collection and preparation is reduced, although fine-tuning may still require carefully curated datasets.[530] Developers can control the data used for adaptation, but they

523 Semi-supervised learning utilises both labelled and unlabelled data. It works well, for instance, with high volumes of data, not all of which can be labelled (Wiggers 2024; van Engelen and Hoos 2020).

524 In unsupervised learning, the algorithm is only provided with raw input data, and the algorithm aims to find regularities therein, to learn to act in unforeseen situations. (Alpaydin 2020, 11). Unsupervised learning could be more capable of finding unexpected, novel patterns that are invisible to its developers, as it is not constrained by predefined labels or outcomes (Hildebrandt 2015, 24; Wiggers 2024).

525 Reinforcement learning is a training method in which the algorithm is provided with the ability to learn from experience. Reinforcement algorithms are programmed to seek incentives (rewards or punishments), and then they are provided with the incentives when they have performed (or not) as the developers wished. See, e.g., (Gerrish 2018, 91–92; Alpaydin 2020, 12). Reinforcement learning could also be done with human feedback (Bai et al. 2022).

526 (Alpaydin 2020, 3; Amershi et al. 2019, 293).

527 (Amershi et al. 2019, 293; ICO 2023, 124; Silva and Alahakoon 2022, 8).

528 For example, inaccurate or biased labelling could lead to breaching the GDPR Art. 5 principles relating to processing of personal data and the Non-Discrimination Directives' prohibitions of discrimination. See, e.g., (Ojanen et al. 2022, 9, 19 and 58–62; ICO 2023, 119). Furthermore, collecting personal data without lawful grounds for processing can breach data protection laws (EDPB 2024c, 4), and relying on biased historical datasets can embed discrimination into the system.

529 For comparisons of different adaptation strategies, see, e.g., (Rodrigues 2024, 105–11; Ohm 2024).

530 See, e.g., (Ohm 2024, 224; Rodrigues 2024, 106).

cannot influence the original training data of the base model,[531] which is typically less processed than the datasets created for recruitment-specific AI systems.[532]

When the developers consider the model ready, the AI recruitment system proceeds to the *verification and validation* phase. In this phase, its performance is tested with unseen data to evaluate, among other characteristics, its accuracy, robustness, and fairness.[533] Metric-based validation may not be sufficient for uninterpretable and indeterminate GPAI-based recruitment systems, which could require systematic auditing of outputs across various prompts to evaluate, for example, fairness.[534] If the model fails to meet the required standards, it may be returned to any of the previous steps for further refinement.[535] The verification and validation phase offers an opportunity to detect and mitigate underlying biases before deployment.[536]

Deployment includes the launch and initial configuration of the system within the recruitment environment.[537] Before launching, employers should ensure that the system complies with all the relevant legal requirements[538] and fulfils its intended purpose, such as unbiased recruitment processes or improved hiring efficiency. If multiple recruitment systems are used simultaneously, specific coordination is required to ensure compatibility and security.[539]

During *operation*, AI recruitment systems should be continuously monitored to ensure they function reliably and in accordance with applicable laws.[540] Some defects, biases, or inefficiencies in the system's operation may only become apparent

531 The General-Purpose AI Code of Practice, published in July 2025, instructs GPAI providers to only issue certain information on the training, testing and validation data (e.g. data type/modality, data provenance, how it was obtained, number of data points, scope and main characteristics, data curation methodologies and measures to detect unsuitability and identifiable biases). See (Oliver and Bommasani 2025; Peukert and Castets-Renard 2025; Samwald et al. 2025).

532 See, e.g., (Ohm 2024, 225–26).

533 See, e.g., (Viljanen 2022, 319). AIA Art. 9(8) permits testing to be conducted at any time during the development process, provided it is done before the system is placed on the market. It could also be beneficial to include lawyers in this phase and not leave the testing solely to engineers or business professionals.

534 See also (Viljanen 2022, 317).

535 (Amershi et al. 2019, 292).

536 (ICO 2023, 124–25).

537 See, e.g., (Silva and Alahakoon 2022, 8–9).

538 See section 5.2 below.

539 Of the use of multiple systems, see, e.g., (Bogen and Rieke 2018, 14).

540 (UK National Cyber Security Centre and US Cybersecurity and Infrastructure Security Agency 2023, 16; ICO 2023, 128; OECD 2024, 8). See AIA Arts. 14 and 26, and GDPR Art. 35(11), that could practically extend the monitoring requirement also to ADM, even when conducted by other than AI systems.

during real-world use.[541] Regular audits are therefore essential for detecting such problems and implementing necessary updates or retraining.[542] The lifecycle of an AI recruitment system concludes when it is decommissioned or replaced[543], though its social and organisational impacts may persist beyond its technical retirement.

Multiple actors are involved in the lifecycle of the AI recruitment system. As noted in section 2.5, employers may purchase the systems from specialised providers that develop ARSs.[544] Hence, the providers' decisions can affect the recruitment process and compliance with legal requirements.[545] However, in addition to adopting off-the-shelf products with limited control over their design or development, employers may also actively participate in the early stages of the ARS's lifecycle to obtain tailored solutions. Providers may also incorporate components from third parties,[546] which creates complex supply chains that complicate compliance and the attribution of liability for potential damages.[547]

With the GPAI-based recruitment systems, this complexity intensifies. Large external providers typically develop the base models, while downstream providers or employers themselves may adapt them for recruitment purposes.[548] Consequently, the responsibility for compliance is also fractured: the GPAI provider controls the pretraining phase, while those adapting the GPAI model control the recruitment-specific implementation. For instance, non-discrimination and data protection matters must be noted at all levels to ensure compliance. Allegedly, some biases might be fixed when adapting the GPAI models to recruitment tasks.[549] However, the EDPB has considered that unlawful processing of personal data during the development of an AI model may also affect entities that use systems built on that model.[550]

541 (ICO 2023, 128). See also AIA Recital 91.
542 (ICO 2023, 128).
543 (ICO 2023, 133).
544 (ICO 2023, 74; Bogen and Rieke 2018, 14; Cristofolini 2024, 86; Yusifli 2024, 229). There are various ways in which the systems may be accessed, including 'as a service' or 'off-the-shelf', see, e.g., (Barberá 2025, 27; Cobbe and Singh 2021).
545 See, e.g. (Cristofolini 2024, 86).
546 (Raghavan et al. 2019, 12). *Manish Raghavan et al.* mention facial analysis software as an example of third-party-supplied software in hiring systems. See also AIA Art. 25(4) and Recitals 88–90.
547 See also (Raghavan et al. 2019, 12; Cobbe et al. 2023).
548 With vibe coding tools, employers could also increasingly develop the systems themselves, even if they have no development experience and only limited expertise. This combination is likely to increase legal risks, and employers would often be subject to the AIA's provider obligations.
549 See, e.g., (Ohm 2024, 239–40).
550 (EDPB 2024b, 33–34).

Next, the evolution of the technologies behind the systems will be introduced, covering and comparing especially task-specific systems and LLM-based recruitment systems,[551] as these developments may affect the legal constraints.

3.3 Shift in the technologies behind algorithmic recruitment

3.3.1 Prior task-specific recruitment systems

When I commenced this dissertation project in 2020, recruitment systems were typically designed specifically for that context to analyse available data and predict future recruitment outcomes ('task-specific ARSs').[552] These prior ARSs were often framed in terms of big data[553] and *people analytics* as its employment-specific application.[554] The task-specific ARSs functioned across various phases of the recruitment process, from sourcing and screening to interviewing and selection.[555] These systems were purported to predict various outcomes, such as job applicants' potential job performance, the probability of engaging with a job advertisement, or their likelihood of accepting an offer.[556]

An often-cited example of task-specific ARSs is Amazon's recruitment algorithm[557] which, after being trained on a decade of resumes, systematically downgraded female applicants for technical roles, despite attempts to make the

551 Emerging agentic AI recruitment systems are noted only briefly, given the scarcity of scientific literature on the subject at the time of writing this section.

552 (Bogen and Rieke 2018, 6). Of task-specific models and systems, see, e.g., (Bommasani et al. 2021, 123; Hacker et al. 2025, 2).

553 Various definitions for big data exist. For instance, *Jonathan Ward and Adam Barker* have surveyed the big data definitions, thereafter defining it as 'a term describing the storage and analysis of large and or complex data sets using a series of techniques including, but not limited to […] machine learning' (Ward and Barker 2013). See also (Barocas and Selbst 2016, 673; Bodie et al. 2017, 962; Kim 2017, 864 and 877; WP29 2013, 45).

554 Simply put, people analytics refers to the use of predictive analytics in human resources management, see, e.g., (Peck 2013). For more detailed descriptions of the term, see, e.g., (Bodie et al. 2017, 962–73; Kim 2017, 860–62; Cherry 2016, 7–11; Giermindl et al. 2022, 410–11).

555 (Bogen and Rieke 2018, 13–43).

556 (Bogen and Rieke 2018, 44).

557 For the original report on the Amazon case, see (Dastin 2018). Research and news articles repeatedly refer to it, see, e.g. (Ajunwa 2020, 1673–74; Yin et al. 2024; Aloisi 2024, 56). It is often used as an example in general research discussing the discriminatory potential of algorithms, see, e.g., (Adams-Prassl, Binns, et al. 2023, 147).

system gender neutral.[558] Amazon's infamous recruitment algorithm was designed to work as follows: feed the algorithm with the CVs of job applicants, the algorithm scores and ranks the CVs, and outputs its prediction of the best applicants for the open position quickly.[559]

At the core of the task-specific ARSs was *machine learning.*[560] Algorithms processed training data to generate models that take inputs (e.g., data about applicants' qualifications) and output predictions (e.g., of future work performance).[561] The *training datasets,* while potentially vast and varied, were typically related, at least indirectly, to employment or work performance and were therefore relatively structured and limited in scope.[562] For instance, publicly available sources report that Amazon's system was trained on CVs submitted to it over the past ten years.[563] The resulting models predicted future outcomes, such as whether an applicant would be a good fit for the organisation's culture.[564] A key limitation of such models is their reliance on correlations rather than causation, which can lead to erroneous or biased results.[565]

Task-specific ARSs could leverage diverse *input data* originating from various sources. Job applicants could provide unstructured data, such as CVs, cover letters, and recommendations from previous employers. Additionally, job applicants could provide structured data in their social media profiles and application forms.[566] Furthermore, applicants could undergo assessment through gamified evaluations and psychometric tests, providing additional data points.[567] The *outputs* these task-specific ARSs generated frequently included quantitative indicators, such as numerical scores or rankings, used to shortlist or prioritise job applicants.[568]

The prior task-specific ARSs were relatively simple, despite attracting attention and concern among job applicants. Advances in neural networks, training data,[569]

558 (Dastin 2018). According to Dastin, the project started in 2014 and ended early 2017. The algorithm, for instance, downgraded applications that contained word 'women's'.

559 (Dastin 2018).

560 There are numerous different types of machine learning algorithms, the following is only one example. See, e.g., (Alpaydin 2020; Domingos 2012).

561 (Bogen and Rieke 2018, 6; Kleinberg et al. 2018, 115).

562 (Kim 2017, 860–62; Bogen and Rieke 2018, 44). However, as *Pauline Kim* points out, the data also included information about job applicants' attributes and behaviours, which might not be directly related to the employment relationship.

563 (Dastin 2018).

564 (Bogen and Rieke 2018, 7).

565 (Kim 2017, 865–66, 875, and 880–81).

566 (Sánchez-Monedero et al. 2020, 2).

567 (Sánchez-Monedero et al. 2020, 3).

568 (Bogen and Rieke 2018, 6).

569 How the whole business model of the big technology companies has been formed for this purpose of collecting data, see (Zuboff 2019).

and computing power[570] have enabled more complex ARSs that incorporate deeper learning and enhanced natural language processing (NLP)[571] capabilities.[572] These developments, though gradual, became widely visible to the general public with the release of ChatGPT.[573]

3.3.2 Contemporary LLM-based recruitment systems

When initiating the writing of this synthesis in late 2024, state-of-the-art recruitment solutions purportedly increasingly relied on generative AI.[574] Generative AI encompasses models that learn patterns from training data and, in response to prompts, can create new content such as text, pictures or audio.[575] Within the recruitment domain, LLMs, known for their ability to generate text-based outputs, appeared particularly promising.[576] Thus, LLM-based recruitment systems are examined in this dissertation as an example of generative AI solutions within the recruitment context.

LLM-based recruitment systems leverage general-purpose base models[577] such as GPT-5 or LLaMA, which can perform a range of general tasks.[578] LLMs are initially trained to predict the most likely text string in response to a prompt.[579] However, their large scale and architecture allegedly generate broader capacities,

570 See, e.g., (Sevilla et al. 2022).

571 Natural language processing denotes the automation of natural language functions such as 'analysing, producing, modifying, or responding to human texts and speech', see (OECD 2023, 14). In the field of NLP, the creation of the 'Transformer' architecture by Vaswani et al. in 2017 marked, purportedly, a significant advancement that empowered large language models, see (Vaswani et al. 2017; OECD 2023, 23).

572 (OECD 2023, 22; Hacker et al. 2023, 1113; Bommasani et al. 2021, 4; Bowman 2023, 2).

573 For a more detailed description of the history of these systems, see, e.g., (Cao et al. 2023; Bommasani et al. 2021, 9). Two months after its launch, ChatGPT was credited with reaching 100 million monthly users, making it the fastest-growing consumer application (Hu and Hu 2023). In November 2025, OpenAI claimed that ChatGPT already had more than 800 million weekly users and 1 million business customers worldwide (OpenAI 2025a). Of the significant increase in adoption of AI at work since the release of ChatGPT, see also (Gillespie et al. 2025, 69).

574 (Broad 2024). See also (Walker and Larson 2025).

575 (Feuerriegel et al. 2024, 111). See also (Hacker et al. 2023). On the use of generative AI in the employment context, see, e.g., (Söllner et al. 2025).

576 See, e.g., (Heymans 2024; Hirize 2024).

577 Others have referred to these as foundation models, see, e.g., (Bommasani et al. 2021, 7).

578 (Almada and Petit 2023, 14).

579 See, e.g., (Mittelstadt et al. 2023, 1831; Ohm 2024, 223; Kambhampati et al. 2025, 2; Hao et al. 2024, 1; Grzankowski et al. 2025, 5). For criticism of this framing, see, e.g., (Grzankowski et al. 2025).

including coherent text generation and even reasoning.[580] Thanks to their large scale and extensive training data, LLMs can allegedly model more complex linguistic relationships and create internal representations of the world, enabling them to infer the nuances of natural language more accurately.[581]

Researchers do not fully understand the inner workings of these highly complex LLMs[582] and those demonstrate powerful emergent capabilities.[583] Yet, it is widely recognised that larger models with more extensive training data tend to perform better in language processing.[584] The most advanced, high-capability LLMs, such as GPT-5 or Gemini, are vast neural networks; however, their exact technical details remain unknown to the public.[585] Meta's open-source large language model Llama 3.1 is stated to have 405 billion parameters[586]. LLMs are trained on wide, diverse data comprising various topics, languages, and styles.[587] However, the training datasets could be scraped from Internet sources,[588] which often include biased, harmful and inaccurate content,[589] making LLMs susceptible to replicating such issues, especially if robust safeguards are not implemented.[590]

580 See, e.g., (Hao et al. 2024; Kambhampati et al. 2025; Patil 2025, 2; Grzankowski et al. 2025, 8–9). See also (Bowman 2023, 4–5) and the sources cited therein.

581 I do not mean this in the sense that the LLMs would exhibit human-like understanding. But rather that they are able to group, for instance, certain words consistently together, such as 'rain' and 'wet'. According to Bowman, this capability allows the systems to reason on an abstract level (Bowman 2023, 4–5).

582 See, e.g. (Ohm 2024, 238–39).

583 For instance, the chain-of-thought reasoning (i.e., the capability to explain its reasoning pattern when answering questions) is one of such emergent capabilities which the developers had not intended and which appeared in use (Bowman 2023, 8; Wei et al. 2023). See also (Bommasani et al. 2021, 1 and 6; Hacker et al. 2025, 3).

584 (Kaplan et al. 2020, 3; Bowman 2023, 1–2).

585 The technical details of GPT-4 also remained unknown to the public (Heaven 2023). GPT-3 was stated to have 96 layers and 175 billion parameters in its neural network (Li 2020).

586 (Llama Team, AI @ Meta 2024). For comparison, the Chinese competitor Deepseek-V3 model is stated to have a total of 671 billion parameters, see (DeepSeek-AI et al. 2025, 1).

587 See, e.g., (Bommasani et al. 2021, 122; Guinness 2024).

588 See, e.g., Common Crawl (2024), which provides a web data archive for training models. Several legal issues are associated with training data scraped from online sources. For instance, *Taner Kuru* has assessed the lawfulness of using publicly accessible online data to train LLMs from the perspective of the GDPR, discussing both the lawful basis of legitimate aim and the processing of sensitive personal data, as well as whether it has been made manifestly public (Kuru 2024). Copyright issues are also significant. Several cases of copyright infringement have been brought against major technology companies developing LLMs, and copyright issues have also been widely discussed in prior research, see, e.g. (Gervais et al. 2024; Novelli et al. 2024).

589 (Luccioni and Viviano 2021).

590 See, e.g., (Dong et al. 2024, 5–9).

To apply LLMs in practice, further adaptations or guidance are often necessary.[591] General-purpose adaptations, such as the ChatGPT general-purpose conversational system built on GPT-5, enable LLMs to generate content, create summaries, analyse documents, and translate languages.[592] These systems could also assist with various recruitment tasks.[593] However, from the perspective of accuracy and non-discrimination, it is ostensibly preferable to fine-tune the GPAI models or systems for recruitment-specific tasks.[594] Accordingly, this dissertation focuses on LLM-based recruitment systems developed through fine-tuning, tailoring them specifically for recruitment needs.

In fine-tuning, the pretrained base model is adapted to specific tasks or domains while retaining its broad general capabilities.[595] Apparently, the capabilities of the fine-tuned models 'can be more targeted, specialised, or nuanced' than those of the original base model.[596] The LLM-based recruitment systems can be adapted to perform diverse recruitment-specific tasks, such as generating job advertisements, answering job applicants' queries, and screening and interviewing candidates.[597] This approach allows LLMs to utilise their general linguistic capabilities and broad factual knowledge base while addressing specific recruitment needs.[598]

591 (Bowman 2023, 5). However, not necessarily big adaptations are required. According to Bowman, typical ways to adapt the LLMs include plain language model prompting (e.g. providing the model with a task, which it can solve by providing the next word in a text), supervised fine-tuning (offering human examples to train the model) and reinforcement learning (human users to give positive or negative feedback on the model's behaviour to guide it to the desired direction).

592 (Hacker et al. 2023, 1114).

593 According to OpenAI, organisations using ChatGPT often fine-tune the model to mitigate biases further (Yin et al. 2024). However, there is a risk that this fine-tuning to use the general-purpose AI model in the recruitment context may make the deployer a provider under the AIA, see AIA Art. 25(1)(c) and discussion above in sections 2.5 and 3.2.

594 See, e.g. (Bommasani et al. 2021, 17). For instance, in the case of GPT-5, the recruitment-specific solution could be built either on top of the base model GPT-5 or its general-purpose adaptation, the ChatGPT. From the perspective of the employers' compliance obligations, the safest option could be to acquire a fine-tuned system from a third-party provider as it would reduce the employer's risk of being considered a provider under AIA Art. 25. If the system would already be fine-tuned, the developer of the fine-tuned system would be the provider and the employer would more clearly be the deployer under AIA Art. 3.

595 (Ohm 2024, 223; Ji et al. 2023, 7).

596 (Ohm 2024, 223). See also (Ji et al. 2023, 7)Yet the fine-tuned model is intended to preserve the base model's general functionality and basic capabilities, such as its ability to process natural language (Ohm 2024, 217–18).

597 For a few practical use cases of GPT-4 in recruitment, see (Bersin 2023). On the possibilities of fine-tuning, see (Ohm 2024, 223 and 228).

598 See also (Almada 2022, 4; Ohm 2024, 231).

Compared to task-specific ARSs, fine-tuned LLM-based recruitment systems exhibit certain advantages. While task-specific ARSs typically require the separate development of both language and domain knowledge, fine-tuned LLMs efficiently inherit the base model's general capabilities and require only additional recruitment-relevant data to refine their capabilities. This distinction suggests that fine-tuning might be somewhat faster and allegedly easier than developing a task-specific ARS from scratch.[599] Furthermore, LLMs can generalise knowledge across domains, enabling LLM-based recruitment systems to handle more varied input, such as interpreting unconventional CV formats or assessing non-traditional skills from free text. For instance, LLM-based recruitment systems can allegedly infer from the CV text that the applicant possesses a certain competence, whereas task-specific models are more reliant on identifying specific keywords in the documents to find a match.[600]

Despite the advantages, LLM-based recruitment systems also introduce unique challenges. One notable concern is the phenomenon of confabulations[601] (often referred to as hallucinations[602]), where LLMs generate content that may appear plausible but is actually nonfactual, inaccurate, illogical or irrelevant to the provided prompt.[603] Various causes of confabulations have been identified in prior research, including training data and shortcomings in training and inference processes.[604] Confabulations range from obvious mistakes to subtle inaccuracies,[605] that can easily go unnoticed when humans do not thoroughly review all the information the system processes. Real-life incidents where individuals have been wrongly depicted as criminals are an alarming example, highlighting the harm that confabulations could cause to job applicants.[606]

599 (Almada 2022, 4; Ohm 2024, 231). For comparison, see also (Kaplan et al. 2020, 3; Bowman 2023, 1–2).

600 See, e.g. a LLM-based resume parser, which claims to offer a deep understanding of the candidate profiles (Hirize 2024; Bersin 2023).

601 See, e.g., (Smith et al. 2023; Watson 2025). According to *Andrew Smith et al.,* the psychiatric concept of confabulation 'refers to the generation of narrative details that, while incorrect, are not recognized as such'. The confabulations are often linked to a lack of awareness of one's deficits.

602 In this dissertation, the term confabulation is used instead of hallucination. It has been suggested that referring to hallucinations to describe defects in the systems is also an intentional choice that might obscure the technological realities and potential harms, and instead promote a mythology, see (Klein 2023).

603 (Huang et al. 2024, 2; Novelli et al. 2024, 13; Dong et al. 2024, 5; OECD 2023, 10).

604 (Huang et al. 2024, 7–12). For discussion on the causes of confabulations, see also (Novelli et al. 2024, 13; Dong et al. 2024, 5).

605 (Wachter et al. 2024, 2).

606 (Kelsey-Sugg and Carrick 2024). ChatGPT has also been found to have a tendency to fabricate lawsuits, see (Belanger 2023).

To mitigate such risks and improve the accuracy of LLM-based recruitment systems, for instance, a technique known as Retrieval Augmented Generation (RAG) can be employed.[607] In essence, RAG is an architectural pattern where relevant knowledge is sought from external databases (retrieval) and added as contextual information to the prompt before the LLM answers the query (generation).[608] RAG enables LLMs to utilise external databases for additional updated and contextually relevant information, which could ostensibly improve the accuracy and relevance of LLM-based recruitment systems' predictions, reduce confabulations and outdated information, and enhance decision traceability.[609] In recruitment, the external database could consist of employer-specific materials, such as company strategies, mission and value statements, staff policies, performance metrics, job descriptions, and candidate information, including CVs, applications, annotated interviews, and test scores. When using RAG, external databases provide the required contextual customisation, reducing the need for employer-specific adaptations. Updating external databases is also easier than retraining or retuning the model, helping ensure the system stays up-to-date and delivers more accurate outputs.[610]

To sum up, LLM-based recruitment systems could support tasks similar to those of task-specific ARSs and also handle generative assignments throughout the recruitment process. The LLM-based recruitment systems can allegedly process unstructured input data like resumes, CVs, and interview transcripts to generate targeted output such as job advertisements, targeted interview questions, and real-time conversations with job applicants,[611] summaries of job applicants' profiles, analysis, and even scores or rankings. Nevertheless, careful consideration must be given to their limitations, including biases, confabulations, and the potential for reproducing harmful or outdated content.

3.3.3 Emerging agentic AI recruitment systems

The next generation of ARSs is likely to incorporate more agentic AI capabilities. The use of agentic AI in human resources, including recruitment[612], is expected to

607 It is still unclear whether confabulations will ever be completely eliminateable, see, e.g., (Huang et al. 2024, 2; Banerjee et al. 2024, 1).
608 (Casu 2024).
609 (Gao et al. 2024; Robbins 2024).
610 See, e.g., (Gao et al. 2024; AWS 2024).
611 (Heymans 2024).
612 For instance, *Chengguang Gan et al.* proposed using LLM Agents to enhance resume screening processes (Gan et al. 2024).

expand in the near future.[613] At the time of writing, no unified definition of agentic AI systems exists. In this dissertation, agentic AI systems refer to AI systems that can 'autonomously pursue open-ended objectives by taking sequences of actions in complex environments'.[614] Agentic AI systems vary in form. They may involve multiple autonomous AI agents that work together as a multi-agent system, each performing specific subtasks necessary to achieve the system's overall goal, or they may consist of a single AI agent.[615] Key characteristics attributed to agentic AI systems include greater autonomy and adaptability, as well as the capacity for independent decision-making and long-term planning within their operational context.[616]

Agentic AI systems are designed to operate with higher levels of autonomy, enabling them to make decisions and take actions in pursuit of assigned goals.[617] When given a goal, agentic AI systems attempt to reason and plan a suitable sequence of steps to reach that goal.[618] Autonomous action and decision-making require several capabilities, including breaking overarching goals into smaller tasks, perceiving and interpreting information from the environment, and adapting their plans proactively when new information emerges.[619] These systems often rely on tools that interface with the external environment.[620] The autonomy of agentic AI systems allows them to 'perform tasks without constant human oversight'.[621] Nevertheless, humans remain essential for defining boundaries for agentic AI, selecting tasks to delegate to those, conducting testing, overseeing operations, mitigating risks and maintaining transparency.[622]

613 (Salesforce Research 2025; Kshetri 2025). Salesforce Research surveying global human resource executives in 2025 found that AI agent adoption was forecast to increase by 327% over the next two years. However, the pace and extent of adoption will depend on multiple variables, including regulatory developments and how organisations tackle the various challenges related to agentic system adoption (Chopra 2025).

614 (Watson 2025). See also (Stryker 2025; Borrelli et al. 2025, 7).

615 (Masterman et al. 2024, 2; Stryker 2025; Bhattacharya and Verbert 2025, 2; Fourney et al. 2024). The risks of the agentic AI systems also vary depending on the chosen architecture, see, e.g., (Borrelli et al. 2025, 20–21; Masterman et al. 2024).

616 (Watson 2025). See also (Ackerman 2025, 2)

617 (Watson 2025; Andrews 2025; Stryker 2025). In contrast, the LLM-based systems only respond to the user's prompts by providing outputs. If the output creates a need for action, the user must act on their own.

618 (Borrelli et al. 2025, 10; Masterman et al. 2024, 3; Watson 2025).

619 (Watson 2025; Masterman et al. 2024, 3; Ackerman 2025, 2; Stryker 2025).

620 See, e.g., (Borrelli et al. 2025, 10; Stryker 2025; Masterman et al. 2024, 3–4). Instead, LLM-based recruitment systems cannot call tools.

621 (Stryker 2025).

622 (Andrews 2025; Stryker 2025; Kshetri 2025).

Purportedly, some agentic AI systems are designed to update or adjust their behaviour on the basis of new information and experience,[623] but this is not always the case.[624] Agentic AI systems may also display emergent behaviours, such as producing unexpected or novel solutions or adapting to unanticipated challenges when pursuing the goals.[625] These forms of continuous learning and emergent behaviours can raise compliance concerns regarding, among other issues, predictability, auditability, and control. When compared to LLM-based systems, the agentic AI systems place greater demands on organisations, including more complex data infrastructures, expanded application programming interface (API) integrations, and higher levels of organisational capability, which collectively affect their implementation and governance.[626]

According to existing research, agentic AI has the potential to contribute to various stages of the recruitment process, from sourcing candidates to making final decisions.[627] Prior scholarship has identified resume evaluation and job matching as potential use cases for agentic AI.[628] Specialised AI agents have also been developed to explain hiring decisions to job applicants, provide career guidance, and help applicants prepare for interviews.[629]

However, the practical usability of agentic AI recruitment systems may be subject to significant limitations under EU legislation.[630] The GDPR's restrictions on ADM could impose strict constraints on the use of agentic AI in tasks such as resume screening and recruitment decision-making. Not all use cases are equally sensitive; for example, automated job description drafting and interview scheduling[631] may be less affected by GDPR's prohibition of ADM, although they still raise privacy concerns. For instance, scheduling interviews may require access to a wide range of data, including email, calendar, and messaging applications.[632]

Any processing of personal data by agentic AI systems must comply with the GDPR, including the principles of processing personal data (GDPR Art. 5) and the

623 (Ackerman 2025, 2). See also (Stryker 2025).
624 See (Borrelli et al. 2025, 20).
625 (Ackerman 2025, 2). Of emergent behaviour in multi-agent systems, see also (Andrews 2025).
626 (Ackerman 2025, 2).
627 Of a multi-agent system comprising a sourcing, vetting, evaluation and decision agent, see, e.g., (Pathak and Pandey 2025, 7–9).
628 (Bhattacharya and Verbert 2025).
629 (Bhattacharya and Verbert 2025).
630 Although the framework of the key legal parameters set for using ARSs has not been drafted from the perspective of agentic ARSs, the legal parameters are also relevant constraints for agentic AI recruitment solutions.
631 (Kshetri 2025, 120).
632 See (Barberá 2025, 15).

lawful grounds for processing (GDPR Art. 6). Organisations adopting agentic AI should therefore ensure that processing remains transparent and limited to what is necessary for the specified purposes. These requirements demand particular attention throughout the systems' lifecycle, especially where agentic AI systems autonomously adapt their actions. For instance, restricting which applications the agents are allowed to interact with may be necessary to uphold purpose limitation and to ensure that information about the processing can be provided transparently.[633]

Although agentic AI systems hold promise, their characteristics, such as a high level of autonomy, adaptiveness, and emergent behaviours, can also exacerbate the other problems present in earlier generations of ARSs, such as discrimination risks.[634] Controlling and mitigating these problems in agentic AI systems could also be far more complicated. Hence, the adoption of agentic AI systems in recruitment should be viewed with extreme caution.

Since agentic AI began to emerge more broadly only during the finalisation stages of this dissertation, it will not be examined in detail in the following analysis. However, the results of this dissertation may also be helpful when analysing whether agentic AI systems can be used and what their effects could be in recruitment. Yet, it is likely that the requirements triggered by the use of agentic AI are even more complex and demanding for employers than those discussed herein.[635] Next, the discussion briefly returns to the two earlier ARS generations to highlight their key characteristics and differences, which are essential for evaluating the legality of their use.

3.4 Examining and comparing the key characteristics of task-specific ARSs and LLM-based recruitment systems

In this section, the key characteristics of task-specific ARSs and LLM-based recruitment systems will be compared using *Mika Viljanen's* classification of algorithmic and AI technology features as the theoretical framework.[636] Viljanen has argued that when reducing the social harms of algorithmic technologies, six

633 Of the problem of lack of transparency in AI agents, see, e.g., (Barberá 2025, 39–40).

634 (Stryker 2025; Andrews 2025). *Nell Watson* has categorised the risks and challenges of agentic AI into four categories: unintended optimisation, deceptive alignment, power-seeking behaviour, and value misalignment (Watson 2025).

635 When using agentic AI, employers may at times also be deemed providers under the AIA. See AIA Art. 3, point 3 and 25(1). See also sections 2.5 and 1.3.3 above.

636 (Viljanen 2022). *Nea Lepinkäinen* has previously applied this framework in the context of algorithmic harms (Lepinkäinen 2024, 103).

characteristics of the systems are central[637]: *technological agency*[638]*, complexity*[639]*, uninterpretability*[640]*, non-linear performance*[641]*, indeterminacy,*[642] *and dynamicity*[643]. While initially presented as factors affecting the harm potential of the systems, the same characteristics could also affect the systems' legal implications.[644]

When task-specific ARSs and LLM-based recruitment systems are viewed through Viljanen's classification, differences between these two generations of ARSs emerge. To begin with, in task-specific ARSs, developers retained greater control over the key characteristics, while the decision to adopt an LLM largely predetermines these features. Nevertheless, both ARS generations are heterogeneous, and the boundary between them is blurred.

Technological agency refers to the system's ability to perform the functions it is coded to complete, without requiring human intervention.[645] While both task-specific ARSs and LLM-based recruitment systems typically exhibit some technological agency, the extent of this agency can vary considerably depending on the system design and its intended use (e.g., supporting humans or making automated decisions).[646] Although many ARSs serve only a supportive role on paper,[647] human recruiters may over-rely on their outputs, inadvertently amplifying the systems' technological agency and increasing the risk of erroneous and biased decisions.[648] The sophistication of the outputs in LLM-based recruitment systems, combined with the systems' complexity, may increase automation bias.[649] In the AIA, automation bias is defined as automatic reliance or over-reliance on the

637 (Viljanen 2022, 314; 2023, 1212).
638 See (Hildebrandt 2015, 22–23; Viljanen 2022, 315–16; 2023, 1213; Lepinkäinen 2024, 107).
639 (Viljanen 2022, 316; 2023, 1217–20).
640 See (Miller 2019, 1 and 8; Mittelstadt et al. 2019, 2; Viljanen 2022, 317; 2023, 1220).
641 See (Viljanen 2022, 318; 2023, 1223–24; Lipton 2018).
642 (Viljanen 2022, 318; 2023, 1225–26).
643 (Viljanen 2022, 319; 2023, 1226–28; Chen and Liu 2018).
644 (Viljanen 2022).
645 (Hildebrandt 2015, 22–23; Viljanen 2022, 315–16; Lepinkäinen 2024, 107).
646 (Viljanen 2022, 315–16) There has been considerable debate on whether the human should be held in-the-loop, on-the-loop (Enarsson et al. 2022), or be put out-of-the-loop (Lobel 2024).
647 (ICO 2024, 32; Carter 2024, 351–52).
648 Human recruiters may, for instance, be unable to critically analyse the ARS provided scores and rankings before they are used in recruitment decision-making (Bursell and Roumbanis 2024). Cf. Recruiters might also be algorithm-averse and discount the predictions supplied by ARSs. For algorithm aversion in general, see, e.g., (Prahl and Van Swol 2017).
649 (OpenAI 2023a, 59).

system's outputs.[650] In LLM-based recruitment systems, the broad general capabilities and the arguably reduced control following pretraining, contribute to greater technological agency, in contrast to task-specific ARSs, where developers retain more control over the entire development process.[651]

Complexity is significant in both types of ARS. The task-specific ARSs could already process inhumanly vast amounts of data, run sophisticated machine learning algorithms, and operate as part of intricate processes.[652] Hence, from the perspectives of both job applicants and employers, even task-specific ARSs often appeared opaque and complex.[653] However, for developers, task-specific systems remained testable and more comprehensible[654] than the far more complex LLM-based recruitment systems, which, with trillions of neural connections, are unpredictable even to their developers.[655] This complexity also makes it formidable to predict analytically how the ARSs will work in an actual recruitment situation.[656] The increased complexity also hampers the efforts to examine and test system performance.[657]

Complexity also affects interpretability, that is, the ability to explain the system's underlying logic.[658] Systems are *uninterpretable* if even experts with access to the systems' code and data cannot explain them in a manner that humans can understand.[659] Uninterpretability is a characteristic that distinguishes the two types of ARSs. As seen, for example, in the Amazon case[660], at least some task-specific

650 For this definition of automation bias, see AIA Art. 14(4)(b). Generally, regarding automation bias, see (Skitka et al. 1999).

651 Fine-tuning also requires considerable human effort and control. However, the fine-tuners' abilities to understand exactly how the pretrained LLM works or to alter it are limited, see (Ohm 2024, 238–39).

652 See, e.g., (Bodie et al. 2017, 962 and 1025; Kim 2017, 881, 889–90; Cherry 2016, 7–11).

653 See, e.g., (Giermindl et al. 2022, 423–24; Kim 2017, 881; Burrell 2016).

654 For instance, *Sean Gerrish* has emphasised that neural networks are just computers, meaning that as long as the developers know the weights of the connections between nodes and the inputs, the outcomes are also predictable (Gerrish 2018, 111).

655 Of the increased complexity of foundation models, see, e.g. (Bommasani et al. 2021, 122; Bowman 2023, 6). *Samuel Bowman* has claimed that 'our tools for doing neuroscience on these systems are still weak' (Bowman 2023, 6).

656 (Bowman 2023, 6; OECD 2023, 35).

657 (Viljanen 2022, 316). As discussed above in section 3.3.2, the developers have been unable to forecast the capabilities of LLMs, see (Wei et al. 2023; Bowman 2023, 3).

658 There is no unified definition for interpretability (Lipton 2018, 21). Cf. Of uninterpretability, see, e.g., (Miller 2019, 1 and 8; Mittelstadt et al. 2019, 2; Viljanen 2022, 317).

659 See, e.g., (Miller 2019, 1 and 8; Mittelstadt et al. 2019, 2; Viljanen 2022, 317).

660 See section 3.3.1 above. Another often cited case is the use of the name 'Jared' and 'high-school lacrosse' as screening criteria (Gershgorn 2018).

ARSs could potentially be audited and tested to uncover decision-making rules and explain their logic.[661] However, LLM-based recruitment systems, at least for the time being, resist full comprehension.[662] This uninterpretability of LLM-based recruitment systems complicates error detection and risk mitigation.[663]

Non-linear system performance is another likely differentiator between the two generations of ARS. When the system performance is non-linear, even minor changes in input data could lead to different outputs.[664] While some task-specific ARSs could have exhibited non-linear behaviour (i.e. minor variation in input could lead to disproportionate or unpredictable changes in output),[665] others relied on linear models, where the relationship between input and output variables is proportionate and predictable.[666] LLM-based recruitment systems are highly non-linear: a small change in input can yield vastly different outputs.[667] The non-linearity increases unpredictability and complicates testing the systems, which is essential for controlling the ARSs and ensuring they function as planned.[668] For instance, testing a linear ARS with a dozen CVs with divergent demographics could already reveal some biases that would persist regardless of how many times the test is run. However, with the LLM-based recruitment systems, the test would have to be run hundreds of times before biased tendencies might credibly emerge.[669]

Indeterminacy is also a characteristic that divides the two types of ARS. Indeterminacy refers to the phenomenon where, given the same input, the system produces different outputs.[670] The task-specific ARSs were typically deterministic, meaning that with a single input they always produced the same output.[671] By contrast, LLM-based recruitment systems are inherently stochastic, as they generate

661 Of post-hoc explanations, see, e.g., (Vale et al. 2022).

662 (Bowman 2023, 6; Sison et al. 2024, 4864). Although the providers know how they fine-tune LLMs for recruitment purposes, the effects remain unpredictable as the inner workings of the LLMs are unclear even to the providers.

663 (Viljanen 2022, 317).

664 (Viljanen 2022, 318; Lipton 2018).

665 E.g., ARSs utilising simple neural networks or random forests.

666 See, e.g., (Menon and Rahulnath 2016), which partly uses linear regression.

667 Of non-linearity in general, see (Viljanen 2022, 318; Lipton 2018). For instance, if the applicant would have written 'organise' instead of 'organize' the system could have given a completely opposite output.

668 (Viljanen 2022, 318).

669 See, e.g. (Yin et al. 2024), where GPT 3.5 was asked to rank fictitious equally qualified CVs with demographic distinctions 1,000 times, to test whether it showed bias against certain demographics.

670 (Viljanen 2022, 318).

671 This was one of the task-specific ARSs' main selling points: removing inconsistencies in human recruiters' decisions. See, e.g., (Faliagka et al. 2014).

a wide variety of outputs with the same input.[672] The indeterminacy of LLM-based recruitment systems may challenge efforts to prevent unlawful recruitment outcomes.[673]

Finally, *dynamicity* refers to the systems' independent adaptations during operation.[674] Fortunately for the controlling and monitoring efforts, most systems in both generations are *non-dynamic.* This means that the systems do not learn during use.[675] Nevertheless, the emergent capabilities of LLMs also introduce elements of unpredictability that go beyond the developers' initial control,[676] similar to what is observed in dynamic systems.[677]

	Task-specific ARSs	LLM-based ARSs
Technological agency	+	++
Complexity	++	+++
Uninterpretability	+	+++
Non-linear performance		++
Indeterminacy		++
Dynamicity		

Table 1. Summary of the key characteristics of task-specific and LLM-based recruitment systems.

The key characteristics of task-specific ARSs and LLM-based recruitment systems have been summarised above in Table 1 on a scale of + (present/yellow), ++ (high/orange) and +++ (very high/red).[678] In sum, both generations of ARS demonstrate technological agency and complexity, albeit to different degrees.

672 (Dale 2021, 116; Viljanen 2022, 318).
673 (Viljanen 2022, 319).
674 (Viljanen 2022, 319; Chen and Liu 2018).
675 Yet, both generations of ARSs also appear to contain their exceptions. For instance, some algorithms behind targeted job advertisements are claimed to be dynamic and update in real time based on the feedback they receive (Bogen and Rieke 2018, 44). Arguably, some of the fine-tuned recruitment systems built on top of the LLMs could also be continuously learning based on the data they are fed while used, even though the LLM behind the ARSs is not changing, see e.g., (Hirize 2024).
676 (Bowman 2023, 8).
677 (Viljanen 2022, 319).
678 The table is only indicative and depicts high-level generalisations. There could be considerable variation in these characteristics, also within the generations of ARSs.

Likewise, both types of ARS are often non-dynamic. However, LLM-based recruitment systems exhibit greater unpredictability, reduced interpretability, and indeterminacy, making them more challenging to control as required by EU legislation. In the rest of this synthesis, I use the term *intractability* to describe the LLM-based recruitment systems' quality of being difficult to understand, analyse, predict, control, and challenge due to their complexity, uninterpretability, indeterminacy, and emergent, unpredictable behaviour.

The evolution of the ARSs is also visible in the publications introduced in the next chapter. Publications I and II discuss mostly task-specific ARSs, while Publications III and IV also note LLM-based recruitment systems.

4 Summaries of the Original Publications

4.1 AI Applications and Regulation: Mapping the Regulatory Strata

The first publication of this dissertation, "*AI Applications and Regulation: Mapping the Regulatory Strata*", co-authored with Mika Viljanen,[679] challenged the assumption that AI law was in its infancy.[680] Using two fictional case studies, we demonstrated that, even in 2021, AI applications were already governed by a dense regulatory framework. The case studies served as a foundation for developing a framework for understanding AI law as a stratigraphy comprising five layers with varying density and firmness. The stratigraphy also inspired practical guidance for navigating AI compliance processes.

Through the fictional case studies on recruitment and a COVID-19 contact tracing app, we mapped the existing AI-relevant rules. The recruitment case[681] systematically mapped the rules governing the development and use of AI applications in Finnish recruitment processes. The results suggested that AI-based recruitment tools were embedded within a complex regulatory landscape comprising multiple normative layers. Even though our focus was on Finnish legislation,[682] the

679 I contributed to the design and implementation of the research and to the analysis and interpretation of the results. I was responsible for the case study on recruitment and wrote that part of the manuscript, while Mika Viljanen wrote the case study on the COVID-19 tracking app. I also contributed to writing the introduction, stratigraphy and implications sections of the paper.

680 Back then, several accounts implied a dawn of AI law with only a few statutes and other regulatory instruments governing the development and use of AI applications, see, e.g., (Scherer 2016, 356; Guihot et al. 2017, 385–86, 419). This narrative emphasised AI ethics, see, e.g., (Hagendorff 2020, 100).

681 The recruitment case assumed that an automotive assembly company based in Finland intended to employ 400 new employees within a few weeks with the help of an AI-based tool. The AI tool was used to help source applicants, screen applications, test applicants, and analyse video interviews (Publication I / Viljanen and Parviainen 2022, 2).

682 For more detailed discussion on the numerous Finnish Acts governing AI-based recruitment tools, see (Publication I / Viljanen and Parviainen 2022, 2–4).

mappings revealed that AI applications in recruitment were already constrained also by a variety of EU legal instruments, including the Charter of Fundamental Rights, the GDPR, and the Non-Discrimination Directives.

To make sense of the complexity of the regulatory landscape, we proposed a stratigraphy of AI law comprising five distinct but interacting strata: (i) *data rules* regulating data use and posing the first feasibility hurdle, such as the GDPR and trade secrecy rules; (ii) *application-specific AI rules* targeting specific AI applications or application domains, such as the AIA; (iii) *general AI rules* applicable to a wide range of AI applications, such as the GDPR Article 22 qualified ban on automated decision-making; (iv) *application-specific non-AI rules* applicable to specific activities but not to AI specifically, such as co-operation negotiation rules; and (v) *general non-AI* rules that apply generically and across domains, such as fundamental rights, criminal law and liability rules. When viewed through the lens of the stratigraphy, AI law appears as a fragmented and complex patchwork of rules, characterised by varying scopes, regulatory targets, and modalities.

Based on the case studies and heuristic stratigraphy, detailed individual legal rules emerged as the appropriate unit of analysis when considering the content of AI-related law and its impact on the development and use of AI systems. Nevertheless, wide-ranging surveys of legislation and application-specific legal analysis are required, as the application domain crucially affects the regulatory intensity and the scopes of the relevant rules vary significantly. Moreover, we highlighted that much of the legislation governing AI remained emergent, and its precise content and legal effects remain uncertain until a more developed body of case law is established.

These insights also led this dissertation to adopt a holistic approach to the regulation of ARSs, as examining only certain rule complexes would provide a partial and potentially severely misleading picture of the compliance requirements for ARSs and of job applicants' legal protection. Moreover, the results of Publication I also highlighted the need to consider the recruitment context separately from the general employment context.

Publication I addressed the first research question, demonstrating that EU law constrains the use of AI and algorithmic decision-making in recruitment, among other instruments, through data protection and non-discrimination legislation. While Publication I provided a foundational exploration, it did not deliver a detailed legal analysis, reserving that depth for the subsequent publications and this synthesis.

4.2 Can algorithmic recruitment systems lawfully utilise automated decision-making in the EU?

True to its name, Publication II, titled "*Can algorithmic recruitment systems lawfully utilise automated decision-making in the EU?",* examined employers' possibilities

to utilise automated decision-making in recruitment. The article explored three subquestions: 1) Is GDPR Article 22 a prohibition or an enforceable right? 2) What is prohibited ADM in algorithmic recruitment? and 3) Could ADM be exceptionally allowed in recruitment?

At the time of writing, the interpretation of GDPR Article 22 remained unclear, with uncertainty over whether it should be understood as a prohibition or an enforceable right. I proposed that the prohibition interpretation, which sets stricter legal boundaries for ADM and provides a higher level of protection, seemed to be the more appropriate approach in the algorithmic recruitment context.[683]

Further, in Publication II, I supported the interpretation previously advanced by several scholars,[684] that prohibited ADM under GDPR Article 22 should be defined according to the following three criteria: (i) a decision is made, (ii) which is based solely on automated processing, and (iii) which has legal or similarly significant effects on the data subject.[685] I proposed a broad, teleological interpretation of these criteria specifically within the context of algorithmic recruitment. Accordingly, I argued that: (i) interim actions, such as applicant rankings or screenings, should count as decisions; (ii) processing may be considered solely automated also when humans are only nominally involved and do not actively affect the outcome of decision-making; and (iii) decisions significantly affecting applicants' opportunities to proceed in the recruitment process could constitute similarly significant effects. Finally, I emphasised that if any stage of the recruitment process involves automated decision-making, the employer must assess whether an exception under GDPR Article 22(2) permits its use.

In the absence of EU-level authorising legislation, only the contractual necessity and explicit consent exceptions under GDPR Article 22(2) were possibly applicable to algorithmic recruitment. I proposed a teleological interpretation of the contractual necessity exception, which aimed to balance the varying purposes of the provision, permitting employers to invoke it where processing applications manually by other, less privacy- and rights-intrusive means would be practically impossible or unreasonable. Regarding the explicit consent exception, I concluded that, while it is theoretically a possible justification, the power imbalances and information deficits

683 After the publication of the article, the CJEU issued its judgment in *Schufa*, its first case clarifying GDPR Article 22, confirming that the provision should indeed be interpreted as a prohibition. C-634/21 *Schufa*, para 52. See also AG Pikamäe's Opinion in Schufa, para 31. Of later commentaries on the topic, see also (Aza 2024, 11).

684 These three criteria had been identified in prior research, see (Bygrave 2020, 532; Brkan 2019a, 99; Dreyer and Schulz 2019, 11).

685 This division was later confirmed by the CJEU in case C-634/21 *Schufa*, para 43. However, unlike what I had proposed, the Schufa judgement suggested that the criteria could be filled in different steps of the decision-making process, see paras 48 and 73.

make it unlikely that job applicants' consent will meet the GDPR's validity requirements.[686] Even if the applicant's consent were deemed valid in exceptional circumstances, the applicant always has the right to withdraw their consent, rendering the explicit consent exception a faltering basis for ADM.

Ultimately, I concluded that although GDPR Article 22 does not completely prohibit ADM in recruitment, its scope of practical application is fairly limited. Further, I brought up in the conclusions that, in addition to the GDPR, other legislation sets legal boundaries that may restrict the use of ARSs. The AIA's information obligations broadened during the legislative process, and unlike what I anticipated in the conclusions of Publication II, the AIA also sets information obligations for employers as deployers.[687] Nevertheless, as the AIA does not prohibit ADM, GDPR Article 22 remains one of the main constraints for ADM in recruitment, as I suggested in Publication II.

Consequently, Publication II addressed the first research question by analysing the constraints GDPR Article 22 imposes on ARSs. Furthermore, the analysis offered insights into the legal safeguards provided to job applicants.

4.3 Challenges of Direct Discrimination in Algorithmic Recruitment – Insuperable or Not?

In Publication III, "*Challenges of Direct Discrimination in Algorithmic Recruitment – Insuperable or Not?"* I continued examining the legal constraints imposed on AI and algorithmic decision-making, with a focus on non-discrimination. The article investigated whether the prohibition of direct discrimination under EU law[688] can effectively address the challenges posed by ARSs. Scholars had broadly agreed that the EU Non-Discrimination Directives apply to algorithmic discrimination.[689] However, many had doubted the practical utility of the prohibition on direct discrimination, particularly because it faced difficulties in addressing proxy[690] discrimination[691] and the evidentiary burden placed on job applicants.[692] Drawing on previous research by *Jeremias Adams-Prassl et al.*, which had already questioned the dominance of indirect

686 GDPR Art. 4(11), 7 and 22(2)(c).
687 See section 5.2.3 below.
688 See RED Art. 2(2)(a), EED Art. 2(2)(a) and GED Art. 2(1)(a).
689 See, e.g., (Hacker 2018; Borgesius 2020; Gerards and Xenidis 2020; Xenidis and Senden 2020, 166; Wachter et al. 2021, 5–6; Kelly-Lyth 2023; Kullmann 2019).
690 As was discussed in section 3.2 above, a proxy is a neutral feature that is inseparably linked to a protected ground.
691 (Weerts et al. 2024, 1851; Rigotti and Fosch-Villaronga 2024, 5).
692 (Gerards and Xenidis 2020, 67, 70–71; Hacker 2018, 1153; Xenidis and Senden 2020, 172; Martínez-Ramil 2022, 3; Wachter et al. 2021, 20; Carter 2024, 26; Rigotti and Fosch-Villaronga 2024, 5).

discrimination in algorithmic contexts,[693] I analysed whether the challenges posed by proxy discrimination and the evidentiary burden are insurmountable in the algorithmic recruitment context.

First, I examined whether proxy discrimination, where a seemingly neutral feature serves as a substitute for a protected ground, could constitute direct discrimination. To qualify as direct discrimination, job applicants should be treated less favourably than other job applicants in a comparable situation because of their protected grounds.[694] Based on CJEU case law, I argued that direct discrimination can occur even when the less favourable treatment does not formally rest on the protected grounds.[695] Consequently, I concluded that proxy discrimination might also comprise direct discrimination (i) if the proxy is inextricably linked to the protected ground[696] or (ii) if the protected ground has determined the decision to impose the less favourable treatment[697].

I proposed that an inextricable link does not require 100% correspondence between the proxy and the protected ground. Instead, an inextricable link could also exist when the proxy affects persons not in protected groups or only a subset of the protected group, as long as the proxy entirely excludes a protected group or its specific part. Nevertheless, I assumed that finding an inextricable link requires that the proxy is comprehensible and detectable. Previous research suggested that humans often struggle to identify and comprehend proxies.[698]

However, based on prior scholarship and CJEU judgment in Chez, I explored whether complex proxies in opaque systems, such as those built on LLMs, might be considered direct discrimination if it can be shown that the protected ground has been determinative in the recruitment process. That might be the case, for instance, if protected grounds are reflected in the training data and affect the choice of variables that lead to the decision. Nevertheless, I suggested that the more complicated the ARS, the more difficult it is to present the facts, whether under the inextricable link or the determining reasons doctrine.

Furthermore, I endorsed an additional route to tackling proxy discrimination. In the algorithmic recruitment context, the broader, open list of protected characteristics under Article 21 of the CFREU could be applicable, despite the limitations imposed by Article 51(1) of the CFREU. Simply put, the GDPR and the AIA, as directly applicable regulations, could bring algorithmic recruitment within the scope of EU

693 (Adams-Prassl, Binns, et al. 2023).
694 See RED Art. 2(2)(a), EED Art. 2(2)(a) and GED Art. 2(1)(a).
695 See also (Tobler 2022, 78–89; De Vos 2020, 68).
696 See also cases C-267/12 *Hay*, paras 43–44 and C-16/19 *Szpital Kliniczny,* paras 51–53.
697 See case C-83/14 *Chez*, paras 76 and 91.
698 (Cofone 2018, 1413; Prince and Schwarcz 2020, 1281).

law, thereby triggering the applicability of the CFREU, including its Article 21.[699] The broader use of CFREU Article 21 could make it possible to consider more proxies as protected grounds or inextricably linked to protected grounds. However, I found the protection provided by the CFREU to be limited due to the broader justification possibilities and its inability to address situations where proxies remain undetectable.

Second, I examined whether job applicants can realistically meet the burden of proof in direct discrimination cases. Prior research has found it arduous to prove that proxy-based differentiation in ARS is direct discrimination,[700] even though applicants must only 'establish […] facts from which it may be presumed that there has been direct or indirect discrimination'.[701] Theoretically, establishing a prima facie case of direct algorithmic recruitment discrimination requires that the applicants show probable or likely that (1) they are treated less favourably, (2) when compared to another (hypothetical) applicant in a comparable situation, (3) because of their protected grounds. Practically, obtaining evidence of these facts could be difficult. Since the Non-discrimination Directives do not grant the applicants specific rights to information, they must mainly rely on the information disclosures under the GDPR and the AIA.[702]

The evidence needed differs depending on the case and jurisdiction. However, I found that CJEU case law guides national courts to determine the required standard of evidence for job applicants in a manner that ensures a fair allocation of the burden of proof and supports the effective enforcement of the principle of equal treatment among other objectives of the Non-Discrimination Directives.[703] Consequently, I proposed that when determining the required proof, the courts could acknowledge, among other issues, the applicants' reasonable possibilities to provide evidence and how the employers have fulfilled their information duties. Obtaining evidence related to the more complex ARSs is particularly challenging, as is collecting evidence if the employer has breached their information obligations. Hence, I proposed that, for instance, in some cases of complex ARSs, less favourable treatment could be inferred mainly from the results of the ARS. That could eliminate

699 For a more recent analysis on the relationship between the scope of application of the CFREU and AIA, see also (Fink 2025).

700 See, e.g., (Hacker 2018, 1168; Wachter et al. 2021, 6).

701 See RED Art. 8, EED Art. 10 and GED Art. 19.

702 See GDPR Art. 13–15 and AIA Art. 26(11) and 86. Under these regulations, applicants could obtain information, among others, on the role of the ARS in the recruitment process, how it works, which criteria it considers and how relevant those are. For a more detailed discussion on the rights to information see chapters 5 and 6 below.

703 See, e.g., cases C-415/10 *Meister*, paras 39–41, C-109/88 *Danfoss*, paras 13–14, C-104/10 *Kelly*, paras 33–35 and C-127/92 *Enderby*, para 14. See also (Grozdanovski 2021, 117).

the need to detect and analyse the detailed operations of the ARSs. Thus, the burden of proof could be shifted, for instance, if the applicants show that they meet the criteria of the job advertisement, are associated with a protected ground, were not chosen and submission of a similar test application, but without indicia of the protected ground, provided more favourable results.

Publication III demonstrates, in relation to the first research question, that despite its challenges, the direct discrimination prohibition also imposes notable restrictions on AI and algorithmic decision-making, potentially constraining some forms of proxy discrimination. Furthermore, regarding the second research question, Publication III suggests that if a teleological interpretation of the burden of proof provisions is adopted, the direct discrimination prohibition could, at least in some cases, also serve as a practically enforceable safeguard for job applicants' fundamental rights.

4.4 Effective remedies for job applicants in algorithmic recruitment: the contribution of the EU Artificial Intelligence Act

Publication IV, titled *"Effective remedies for job applicants in algorithmic recruitment: the contribution of the EU Artificial Intelligence Act",* continued to examine the remedies available to job applicants. The main research question of the article was whether and how the AIA strengthens job applicants' remedies when algorithmic recruitment breaches their fundamental rights to data protection and non-discrimination. To answer the question, I conducted a legal dogmatic analysis comparing the AIA with the remedies available under existing legal frameworks, specifically the GDPR and the Non-Discrimination Directives. The remedies were considered broadly, reflecting *Giovanni De Gregorio* and *Simona Demkova's* view of remedies under the EU digital acquis,[704] comprising not only judicial remedies but also independent supervision and internal complaints. As informational rights are an essential prerequisite for remedial actions, I also included them in the analysis.

I claimed that the AIA enhances transparency towards job applicants in two ways that could also facilitate their access to effective remedies. First, I argued that the AIA contains measures that could raise job applicants' awareness of high-risk AI recruitment systems. The GDPR explicitly requires informing of ARSs only in case of ADM, while the Non-Discrimination Directives do not require any information disclosures. Under the AIA, employers must notify job applicants if a high-risk AI system is used to make or assist in making decisions about them in the recruitment

[704] (De Gregorio and Demkova 2024).

process.[705] After being informed of the AI use, job applicants could proactively seek information from the EU database for high-risk AI systems. The EU database is likely to contain more extensive information than what the GDPR requires to be disclosed in cases of ADM.[706] Second, the AIA contains an explicit right to an explanation of individual decisions, which also applies when the AI system only supports decision-making.[707] The Non-Discrimination Directives do not contain such a right, and the GDPR provides a right to explanation only in cases of ADM and based on CJEU case law.[708]

Moreover, the AIA offers job applicants an additional avenue for legal recourse, namely the right to lodge complaints with market surveillance authorities.[709] Compared to the GDPR, this right is broader in two aspects, as it also allows legal persons (e.g., trade unions) to file a complaint without the job applicant's mandate or national legislation on the matter.[710] However, under the Non-Discrimination Directives and CJEU case law concerning those, also legal persons have been able to lodge claims in cases where there have not been specific victims.[711] Furthermore, the AIA also appears to enable general complaints regarding compliance, not only complaints related to infringements of job applicants' rights. The market surveillance authorities are likely to have better resources than the job applicants themselves to investigate the potential breaches, which could enhance the effects of this remedial avenue.

Furthermore, the AIA provides new ways to support supervisory authorities' investigations, as the increased documentation and logging requirements generate new types of documentation and information that can assist in investigations (e.g., technical documentation and logs).[712] I assumed that the broader reporting obligations concerning risks and incidents associated with high-risk AI recruitment systems[713] could lead to greater disclosure of system-related problems compared to the GDPR, which requires notification only in cases of data breaches.[714]

Based on the analysis, I concluded that the AIA could strengthen the existing remedies under the GDPR and the Non-Discrimination Directives by providing job applicants, and especially national supervisory authorities, with greater access to

705 AIA Art. 26(11).
706 AIA Art. 71 and Annex VIII Section A.
707 AIA Art. 86.
708 GDPR Art. 15(1)(h) and C-203/22 *Dun & Bradstreet Austria*, para 57.
709 AIA Art. 85.
710 Cf. GDPR Arts. 77 and 80.
711 See e.g., cases C-54/07 *Feryn*, para 25, C-81/12 *Asociata Accept*, para 62, C-507/18 *Associazione Avvocatura per i diritti LGBTI,* paras 39-40.
712 AIA Arts. 11–12.
713 AIA Arts. 20(2), 26(5) and 73.
714 GDPR Arts. 33–34.

information, thereby supporting enforcement efforts. However, beyond the right to lodge a complaint with the market surveillance authority, the AIA does not expand job applicants' administrative remedies. Moreover, judicial remedies for job applicants are also missing from the AIA. Further, the AIA fails to alleviate the evidentiary burden placed on job applicants when challenging unlawful ARS and does not provide concrete remedies, such as compensation for rights violations. Further, job applicants are not entitled to information about serious incidents that have affected them, thereby limiting their knowledge of such incidents.[715] Neither are job applicants offered any internal mechanisms for challenging AI recruitment systems. Furthermore, several structural issues with the AIA limit its effectiveness, such as its limited applicability to existing high-risk AI systems.[716]

However, the protection AIA provides could still be strengthened. Even the informational rights that appeared as the AIA's strength could still benefit from further enhancements. Thus, in Publication IV, I explored a range of solutions to address the shortcomings. Strengthening the AIA's remedies could require, among other measures, clear guidance to facilitate the implementation of the AIA's transparency provisions, such as deployers' information obligations and individuals' right to explanation. Perhaps even more importantly, as the AIA enhancements primarily concern the authorities and their investigatory capabilities, the effectiveness of the remedies requires adequate resources for enforcement. Furthermore, since the AIA permits national measures that are more protective of workers, national legislation and collective agreements may also provide stronger safeguards for job applicants.[717] However, addressing the severest shortcoming, namely the absence of judicial remedies for breaches of the AIA, would necessitate amendments to the AIA's text, if the gap is to be resolved at the EU level. Although such changes appear unlikely now that the European Commission's simplification process is ongoing,[718] they might be considered later when another Commission evaluates the effectiveness of the AIA.

As things currently stand, the AIA could facilitate the use of judicial remedies under the GDPR and the national non-discrimination legislation. However, if the AIA is infringed in isolation, without concurrent breaches of other legislation, job applicants are not explicitly granted a right to an effective judicial remedy under EU legislation. Nevertheless, job applicants might ultimately rely on the CFREU Article

715 AIA Arts. 20(2), 26(5) and 73. Cf. GDPR Art. 34.
716 AIA Art. 111(2).
717 AIA Art. 2(11).
718 (European Commission 2025b).

47, which guarantees them the right to an effective remedy and a fair trial also in disputes between private parties.[719]

Publication IV primarily addressed the second main research question by examining job applicants' remedial safeguards. While focusing mainly on the AIA, the article also reviewed remedies under the GDPR and the Non-Discrimination Directives, thereby providing a broader overview of remedies available to job applicants in the context of algorithmic recruitment.

Taken together, Publications I-IV have provided a basis for systematising the key legal parameters that constrain and shape ARS use. The results of this systematisation will be presented in the following chapter.

[719] C-414/16 *Egenberger*, para 78 and C-715/20 *K.L. v X sp. z o.o*. paras 80–81.

5 Legal Parameters That Constrain and Shape the Use of Algorithmic Recruitment Systems

5.1 Framework of key legal parameters for ARS use under EU legislation

The key legal parameters governing ARS use are scattered across multiple legal instruments and regulatory domains, leading to fragmentation that complicates legal compliance[720] and may weaken job applicants' legal protection. These challenges are further amplified where the applicable rules remain obscure[721] and difficult to interpret, even for the adjudicators. To address these issues, this chapter presents a framework of key legal parameters that systematises how EU legislation across legal fields constrains and shapes ARS use.[722] The framework serves both as a heuristic structure for navigating the complex normative landscape and as an analytical foundation for evaluating job applicants' protection under EU legislation.[723]

The aims and scope of the framework are consistent with those of the dissertation as a whole.[724] Consequently, the framework comprises only legal parameters that directly affect employers'[725] use of ARSs that involve AI or algorithmic decision-making, and are relevant to job applicants' protection against data protection

720 According to *Veronica Root*, the compliance process comprises four stages: prevention, detection, investigation and remediation (Root 2019, 211). Of legal compliance, see also (Lanamäki et al. 2025).

721 In a global study of trust, attitudes, and the use of AI among more than 48,000 respondents from 47 countries, it was found that most people were unaware of the legislation applicable to AI. See (Gillespie et al. 2025, 51).

722 This framework synthesises the analysis presented in Publications I–IV and provides an overview of the relevant EU legislation and legal analysis of the applicable provisions.

723 See Chapter 6 below for analysis of job applicants' protection.

724 See sections 1.2 and 1.4.3 above. For limitations of the framework, see section 1.4.3 above.

725 As mentioned in section 2.5 above, when using ARSs, employers often act as controllers under GDPR Art. 4, point 7 and deployers under AIA Art. 3, point 4. Although the focus herein is on employers, other parties, such as recruitment agencies, may also use ARSs.

infringements and discrimination.[726] The framework primarily incorporates EU secondary legislation, specifically the GDPR and the AIA[727], which bind employers directly, as well as the Non-Discrimination Directives and the Pay Transparency Directive, which affect employers in practice through national implementing legislation that must provide at least the level of protection envisioned in the directives.[728] Moreover, job applicants may invoke certain provisions of the CFREU, such as Article 21 on non-discrimination and Article 47 on the right to an effective remedy, directly against a private employer.[729] However, the CFREU's primary effect on the framework of key legal parameters is that the parameters must be interpreted in conformity with the fundamental rights guaranteed therein.[730]

The framework of key legal parameters is organised along two dimensions: the type of recruitment system to which the legal parameters apply and the type of legal parameters themselves. The rationale behind this categorisation was introduced in section 1.4.3, while this section focuses on its practical application.

The first step in determining the applicable legal parameters is to identify what type of ARS is at hand. The framework distinguishes three main categories of systems: 1) all ARSs[731], 2) AI systems[732] and 3) systems involving ADM[733]. The first

726 Although most provisions relevant for the development phase are left out of the scope of the framework, it includes a few providers' obligations, which could be crucial for employers in demonstrating the lawfulness of ARS use, such as ensuring that only CE-marked high-risk AI recruitment systems are utilised. See section 5.2.2 below.

727 Under AIA Art. 113, many of its relevant provisions are not yet applicable, and further postponement has been proposed as part of the Commission's Digital Omnibus on AI package.

728 See TFEU Art. 288 and section 1.3 above. As noted in Publication I, additional norms within EU secondary law, such as those on trade secrecy, IPR and product liability, can also affect ARSs (Publication I / Viljanen and Parviainen 2022, 4). In the use phase, trade secrets and IPR could be invoked by the employer, for instance, as a reason not to provide certain information in response to a right of access request under GDPR Art. 15(3).

729 See section 1.3.2 above and e.g., C-414/16 *Egenberger*, paras 76–78 and C-193/17 *Cresco Investigations*, paras 76–78. However, for instance, the rights to privacy or data protection have not been assigned horizontal direct effect. See also (Frantziou 2019, 322).

730 See section 1.3.2 above and e.g., C-131/12 *Google Spain*, para 68, C-362/14 *Schrems*, para 38 and C-188/15 *Bougnaoui* para 30. See also (Mast and Ollig 2023, 466–67).

731 See section 2.4 above. For simplicity, the framework assumes that an ARS processes personal data. If that is not the case, the legal parameters stemming from the GDPR would not need to be noted.

732 See section 2.2 above and (Publication IV / Parviainen 2026). The AI system category also comprises a subcategory of high-risk AI systems, among which systems that assist in individual decision-making form a distinct subcategory.

733 ADM has been described as one form of algorithmic decision-making in section 2.3. See also (Publication II /Parviainen 2022, 234–40) and section 4.2.

category is the broadest, as it encompasses all kinds of ARS and all the systems covered by the framework: AI systems and systems involving ADM represent narrower subsets within it. The three categories are not mutually exclusive and frequently overlap, complicating employers' analysis of system type.[734] However, the ARS provider should already have determined whether the ARS is an AI system or a high-risk AI system.[735] Instead, the employer is ultimately responsible for determining whether the ARS is making automated decisions or assisting in such.[736] Furthermore, the type of ARSs may change while in use, further complicating compliance. For instance, if meaningful human involvement in decision-making reduces over time (e.g., due to automation bias), an ARS that initially supported decision-making may become automated, as meant by GDPR Article 22. A similar shift may occur in the context of the AIA, transitioning from a non-high-risk system to a high-risk one if, for example, an AI system initially used only for drafting general recruitment policies is subsequently employed to evaluate job applicants.[737]

Once the type of ARS is identified, the framework of key legal parameters, outlined in *Appendix I,* can be consulted to determine the specific constraints that EU legislation imposes on the use of that ARS. In the framework, the legal parameters have been divided into four main categories: 1) bans, 2) obligations, 3) specific duties, and 4) actionable rights.[738] The chosen categorisation seeks to differentiate the legal parameters on the basis of normative intensity and rigidity, normative target, scope, and the realisation mechanism.[739]

First, *bans* represent legal limits that may not be transgressed. These are further divided into *absolute bans,*[740] which admit no exceptions, and *qualified bans,*[741] which allow derogations under certain conditions. Second, *obligations* encompass

734 As was discussed in section 2.4 above, ARSs may simultaneously constitute AI systems, high-risk AI systems, or involve ADM, or some or none of these. ARSs that are neither AI systems nor use ADM could, for instance, be traditional rule-based systems that only support decision-making in which humans are meaningfully involved.

735 See AIA Art. 6. In such a case, the provider should have fulfilled its duties under the AIA, see AIA Art. 16. See also section 2.5 for examples of situations where employers could become providers under the AIA.

736 This applies both to ADM under GDPR Art. 22, in which case the employer is responsible as the controller and to the decision-making under AIA Arts. 26(11) and 86, as the employer ultimately decides how it will use the ARS and its outputs in decision-making.

737 Of the categorisation of ARS under AIA Art. 6, see section 2.4 above and (Publication IV / Parviainen 2026).

738 Of this systematisation logic, see also section 1.4.3 above.

739 For explanation of these dimensions, see section 1.4.3 above.

740 Absolute bans are marked as red in Appendix I.

741 Qualified bans are marked as orange in Appendix I.

general, often system-level responsibilities that govern either the ARS itself or its use.[742] Third, *specific duties* refer to concrete requirements imposed on employers that demand their proactive measures and arise due to the nature or type of the system deployed.[743] Finally, *actionable rights* comprise legal entitlements that job applicants may invoke in connection with ARS use, the realisation of which depends on their active exercise or enforcement.[744] In the following subchapter, the categories and legal parameters are discussed in the order in which they appear in the framework, without implying a hierarchy of importance.

The following discussion seeks to clarify how the different categories of legal parameters constrain and shape ARS use. Generally, legal parameters with constraining effects prohibit or limit certain designs or behaviours, for instance, by banning specific practices or imposing absolute conditions on ARSs' operations. Instead, legal parameters with shaping effects more flexibly guide the manner in which ARS is to be deployed or its functions. However, the distinction between legal parameters that constrain ARS use and those that shape it is not clear-cut, as the following sections will show. By including legal parameters that both constrain and shape ARS use, the framework is able to depict more comprehensively the legal parameters affecting ARS use, which employers must consider when adopting ARSs. Focusing strictly on legal parameters that constrain ARS use would leave, for instance, the job applicants' actionable rights outside the framework. Hence, to provide a functional analytical basis for the second research question, it is also necessary to include the legal parameters that shape ARS use within the framework. When both aspects are included, the framework also better reflects the multifaceted effects the law has on ARS use.[745]

5.2 Categories of legal parameters

5.2.1 Bans

5.2.1.1 Absolute bans

Bans comprise the legal parameters that determine the prohibited use of ARSs, distinguishing between absolute and qualified bans. Absolute bans are the strictest category of legal constraints set on ARS use, as they explicitly state that some

742 Obligations are marked with yellow in Appendix I.
743 Specific duties are marked with grey in Appendix I.
744 Actionable rights are marked with green in Appendix I.
745 As regards the effects of law, for instance, *Martti Koskenniemi* has described how '[l]aw intrudes everywhere', it does not only 'limit and constrain, more importantly it *empowers* and *enables*' (Koskenniemi 2025, 20).

practice in algorithmic recruitment is not allowed under any circumstances. However, the absolute bans are very narrowly defined, covering only a few highly specific and circumscribed ARS use cases. This category includes the prohibition of asking about pay history and four prohibited practices in AI systems.

Ban on asking about pay history applicable to all ARSs

There is one absolute ban that will soon affect all ARSs: the prohibition on asking applicants about their pay history during their current or previous employment relationship. This ban is outlined in the Pay Transparency Directive (PTD) Article 5(2), which Member States are required to implement by 7 June 2026.[746] Information asymmetries between employers and job applicants regarding pay levels have been identified as a factor contributing to gender- and race-based pay disparities. The ban could tackle these information asymmetries, thus supposedly contributing to more equal pay.[747] However, it remains to be seen how this prohibition is to be implemented, interpreted, sanctioned, and enforced in the Member States.[748]

Even without explicitly requesting previous pay information, ARSs may infer it from other data they process. Considering the purpose of the PTD[749] and its Recital 33, which states that '[e]mployers should not be allowed to enquire or proactively try to obtain information about the current pay or prior pay history of an applicant for employment', the ban could be interpreted to cover ARS-based inferences of pay history.[750]

Due to the ban's high specificity, it will not generally constrain the use of ARSs. Nevertheless, this ban will likely shape the ARSs so that they avoid using pay history as a variable.

Banned practices in AI systems

The most notable absolute bans are outlined in AIA Article 5, which, without exception, forbids harmful manipulation, deception, and exploitation, social scoring,

746 See PTD Art. 34.
747 (Bamberger and Alterman 2024, 43).
748 Member States may provide more favourable provisions to workers (PTD Art. 27).
749 See PTD. Art. 1, according to which it aims to strengthen the principle of equal pay and the prohibition of discrimination, in particular, through pay transparency and reinforced enforcement mechanisms.
750 However, other EU legislation may also constrain such inferences. For instance, GDPR Art. 5 principles of processing, such as the lawfulness, data minimisation and purpose limitation, could restrict the personal data available for such inferences.

untargeted scraping of facial images, biometric categorisation for certain sensitive characteristics, and real-time remote biometric identification systems for law enforcement purposes.[751] However, the relevance of many of these bans to recruitment is likely limited, as is their scope. In addition to the above-mentioned, AIA Article 5 also forbids individual risk assessment and prediction of criminal offences as well as emotion recognition in the workplace, but those bans contain explicit exceptions, making them actually qualified.[752]

Although the use of *subliminal, manipulative, or deceptive techniques* (AIA Article 5(1)(a))[753] as well as practices that *exploit vulnerabilities*[754] (AIA Article 5(1)(b)) presumably are relatively rare in the recruitment context, such practices remain technically possible. Such techniques might appear useful, for instance, if it is hard to find a suitable person for a position with tough working conditions and unappealing pay levels. Yet, the impact of these two prohibitions on potentially manipulative or exploitative AI practices in recruitment could be limited. The prohibitions apply if the objective or effect of the AI practice is to materially distort the behaviour of a person or a group of persons, so that it causes, or is reasonably likely to cause, significant harm.[755] The vague standard of significant harm may weaken the enforceability of these prohibitions.[756] For instance, if the working conditions of the work to be offered nevertheless meet the minimum legal requirements and are non-discriminatory, the employer might claim that even the supposedly manipulative or exploitative AI recruitment practices do not cause or are likely to cause significant harm to job applicants.[757]

Instead, the use of prohibited *social scoring* appears more probable in algorithmic recruitment. To count as prohibited social scoring under AIA Article

751 See AIA Art. 5 and the European Commission's guidance on the prohibitions (European Commission 2025c).

752 See section 5.2.1.2 below.

753 See also (European Commission 2025c, 19–32).

754 The vulnerabilities covered by the provision include only age, disability or a specific social or economic situation, such as persons living in extreme poverty or religious minorities (AIA Art. 5(1)(b) and Recital 29). See also (European Commission 2025c, 34–38; Rebrean and Malgieri 2025).

755 These are common requirements for both bans. In addition to these, for the ban on subliminal, manipulative or deceptive techniques to apply the practice should appreciably impair the ability to make an informed decision, making the person to take a decision that they would not have otherwise taken (AIA Art. 5(1)(a)).

756 The Commission's Guidelines emphasise the case-specific evaluation of the significance of the harm (European Commission 2025c, 30).

757 See AIA Arts. 5(1)(a) and 5(1)(b). The Commission's Guidelines appear to give weight to compliance with other relevant legislation (European Commission 2025c, 32).

5(1)(c), there should be evaluation[758] or classification[759] of person(s) over a certain period of time[760] based on their social behaviour or known, inferred or predicted personal or personality characteristics,[761] with the social score leading to detrimental or unfavourable treatment (i) in a social context unrelated to the context in which the data was originally generated or collected; and/or (ii) that is unjustified or disproportionate to their social behaviour or its gravity. For instance, using credit scores in the recruitment decision-making in a way that negatively affects the decision could presumably trigger the prohibition.[762] In such a case, the credit scores would be the result of an evaluation of the job applicants over a certain period of time, based on their social behaviour and/or personal characteristics, with the social score leading to detrimental treatment in a context not related to the creditworthiness context in which it is originally collected.[763] However, in addition to this literal and protective reading, alternative interpretations also appear.

Although the wording of the AIA does not provide for any exceptions, AIA Recital 31 and the Commission guidelines suggest that EU or national law may still permit specific evaluation practices.[764] Allegedly, there may still be Member State legislation that permits the use of social scoring in employee and job applicant evaluations.[765] However, as AIA Article 2(11) allows national legislation only to the extent that it is more favourable to workers, it could be argued that such national laws are contrary to the AIA if AI systems conduct the analysis and the result is to the detriment of job applicants. If confirmed to exist, such loopholes in what are

758 Commission guidelines state that evaluations include some assessment or judgment about a person. The guidelines cite profiling as a specific example of evaluation (European Commission 2025c, 52).

759 Classification could involve sorting applicants based on known characteristics such as education or age, see also (European Commission 2025c, 52). Hence, the classification criterion also includes measures that do not constitute profiling under GDPR Art. 4, point 4, as profiling requires some form of evaluation of natural persons.

760 Based on the Commission guidelines, the assessment 'should not be limited to a one-time or at once rating or grading with data or behaviour from a very specific individual context', see (European Commission 2025c, 53).

761 See (European Commission 2025c, 54).

762 See also (European Commission 2025c, 52–53, 55). Another example of social scoring used by *Michael Veale* and *Frederik Zuiderveen Borgesius* is automated 'social media background checks' (Veale and Zuiderveen Borgesius 2021, 100).

763 See also (Genicot 2025, 8).

764 AIA Recital 31 states that the prohibition 'should not affect lawful evaluation practices of natural persons that are carried out for a specific purpose in accordance with Union and national law'. See also (European Commission 2025c, 61–62).

765 For instance, in Finland, under Section 5a of the Act on the Protection of Privacy in Working Life (759/2004), employers have the right to process personal credit data of job applicants selected for a position requiring particular reliability, in order to assess their trustworthiness.

nominally absolute bans undermine their effectiveness and normative credibility. Yet, if these loopholes are closed, the prohibition on social scoring could expand the range of situations where scoring job applicants is prohibited.[766] Unlike the ban on ADM, the prohibition on social scoring would then be absolute as its wording suggests.[767]

Finally, the AIA Article 5(1)(g) prohibition of *biometric categorisation systems*[768] that categorise individually natural persons based on their biometric data[769] to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation could also be relevant in recruitment.[770] For instance, an AI recruitment system could technically utilise facial images from social media to infer the person's religion, sexual orientation or ethnicity and target job advertisements based on that information.[771] Such a practice would be prohibited by AIA Article 5(1)(g), along with the constraints set by the Non-Discrimination Directives' prohibitions of discrimination and the GDPR's prohibition of processing special category data.[772]

ARSs do not require these prohibited AI practices to function. Hence, these prohibitions do not categorically prevent the use of ARSs. However, employers must ensure that such practices are not embedded in any phase of the ARS, even as inadvertent effects.[773] Non-compliance with the bans could have serious consequences. In addition to a range of less stringent measures, the market surveillance authorities may demand that operators cease the prohibited practices.[774] If the demand is not met, market surveillance authorities may initiate actions to

766 Of the relationship between the prohibition of ADM under GDPR Art. 22 and the prohibition of social scoring under the AIA, see also (Genicot 2025, 9).

767 Similarly also (Genicot 2025, 9).

768 According to AIA Art. 3, point 40, as biometric categorisation systems are counted 'AI systems for the purpose of assigning a natural person to specific categories on the basis of their biometric data'. However, if the system is 'ancillary to another commercial service and strictly necessary for objective technical reasons', it is not deemed a biometric categorisation system.

769 See AIA Art. 3(34), according to which biometric data is 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data'.

770 The prohibition contains an exception applicable only for law enforcement purposes, see AIA Art. 5(1)(g).

771 For somewhat similar examples regarding political advertising and advertising based on sexual orientation, see (European Commission 2025c, 92–93).

772 Of discrimination in the automated targeting of job advertisements, see (Parodi 2024).

773 While the majority of the AIA's obligations concern only providers, the prohibitions in Art. 5 are operator-agnostic, see also (European Commission 2025c, 5–7).

774 More modest enforcement measures available to authorities include, e.g. warnings and non-monetary measures, see AIA Art. 99(1) and Art. 14 of the Market Surveillance Regulation.

withdraw the ARSs from the market or recall them.[775] There is also a threat of substantial monetary sanctions for breaching the AIA's bans, such as administrative fines of up to 35 million euros or 7% of the undertaking's total worldwide annual turnover for the preceding financial year, whichever is higher.[776] For SMEs, including start-ups, the maximum fine will be the lower of the two previously mentioned amounts.[777]

5.2.1.2 Qualified bans

The category of qualified bans includes norms that, based on their wording, appear to be bans but allow exceptions under certain conditions. Compared to absolute bans, qualified bans have a broader scope. Hence, although the qualified bans may initially appear less stringent than the absolute bans, they could constrain a broader range of ARSs. This category includes prohibitions on discrimination, processing special category personal data and personal data relating to criminal convictions, two types of prohibited AI practices, and automated decision-making.

Qualified bans applicable to all ARSs

The prohibitions of discrimination in the Non-Discrimination Directives and the CFREU apply regardless of the type of ARS, forbidding direct and indirect discrimination of job applicants.[778] However, differences in treatment may be justified under certain circumstances, which makes these bans qualified. Moreover, the Non-Discrimination Directives' prohibitions are limited in their scope.

The Non-Discrimination Directives set out exhaustive lists of protected grounds to which the prohibitions of discrimination apply, including racial or ethnic origin[779], religion or belief, disability, age, sexual orientation,[780] and gender[781]. Yet, several

775 See AIA Art. 79.
776 See AIA Art. 99(3).
777 Unlike under the GDPR, SMEs are subject to lower penalties under the AIA; see AIA Art. 99(6). However, the AIA does not define what counts as an SME.
778 See RED Arts. 2 and 3, EED Arts. 2 and 3, GED Art. 14 and CFREU Arts. 20 and 21. Harassment could also be deemed as prohibited discrimination, if unwanted conduct related to the prohibited grounds occurs 'with the purpose or effect of violating the dignity of a person and of creating an intimidating, hostile, degrading, humiliating or offensive environment', see RED Art. 2(3), EED Art. 2(3) and GED Arts. 2(1)(c) and 2(2)(a). In theory, for instance, ARSs that include chatbots could conduct in a way that would amount to such harassment.
779 RED Arts. 1 and 2.
780 EED Arts. 1 and 2.
781 GED Arts. 1 and 14.

Member States have adopted broader, non-exhaustive lists of protected grounds into their domestic legal frameworks.[782]

In contrast, the CFREU Article 21 prohibits any discrimination based on any ground and explicitly provides for a non-exhaustive list of protected grounds.[783] This list extends beyond those contained in the Non-Discrimination Directives and includes, among others, colour, social origin, genetic features, language, political or any other opinion, membership of a national minority, property, birth, and nationality.[784] Given the possible horizontal direct effect of CFREU Article 21,[785] it may expand the prohibitions of discrimination to cover grounds not stipulated in the Non-Discrimination Directives and broaden the constraining effects of the bans on discrimination, if it is applicable to the ARS use case at hand.

However, as mentioned in section 1.3.2, the scope of application of the CFREU is limited to situations where Member States are 'implementing EU law', that is acting 'in the scope of Union law'.[786] The CJEU has ruled that if a situation, such as recruitment, falls under the ambit of the Non-Discrimination Directives but involves differential treatment based on grounds not explicitly listed in those Directives, it falls outside the scope of EU law, and the CFREU does not apply in such cases.[787] Nevertheless, in Publication III, I proposed a more expansive interpretation, suggesting that when national courts directly apply EU legislation, such as the GDPR, and soon also the AIA, they would act within the scope of EU law. Under this broader interpretation, CFREU Article 21 could become enforceable in algorithmic recruitment scenarios where the GDPR or AIA applies directly.[788] Since at least the GDPR will apply to nearly all ARSs,[789] it is critical for employers to

782 (Publication III / Parviainen 2024, 455; Chopin and Germaine 2023, 11). *Chopin and Germaine* have conducted a comparative analysis of Member States' non-discrimination legislation. For instance, in Finland, the Non-discrimination Act (1325/2014) contains a non-exhaustive list of protected grounds.

783 Similarly, also in ECHR Art. 14.

784 CFREU Art. 21(1). See also (Publication III / Parviainen 2024, 451–55).

785 See section 1.4.2 above and cases C-414/16 *Egenberger*, paras 76–78 and C-193/17 *Cresco Investigations*, paras 76–78.

786 CFREU Art. 51(1) and its Explanations, where the latter formulation appears. For a more detailed discussion on this limitation in the ARS context, see also (Publication III / Parviainen 2024, 451–55).

787 C-354/13 *FOA*, paras 36–39. See also (Publication III / Parviainen 2024, 453).

788 (Publication III / Parviainen 2024, 454). In Publication III, I have discussed the applicability of the CFREU more broadly in non-discrimination cases where decisions rely on grounds other than those listed in the Directives (Publication III / Parviainen 2024, 453–55). On the effects of AIA on the scope of application of the CFREU, see also (Fink 2025).

789 An exception could be, for example, an ARS used solely for drafting general recruitment policies, job descriptions or job advertisements.

ensure that these systems do not discriminate on any grounds listed in the CFREU or closely related ones. Yet, identifying such related grounds in advance is inherently challenging and requires close attention to the evolving EU non-discrimination case law. Where the ARS and the proxies it uses are inscrutable, ensuring that the system does not rely on such related grounds becomes not only highly complex but also, at times, practically impossible.[790]

Under the Non-Discrimination Directives, *direct discrimination* in recruitment occurs if a job applicant is treated less favourably than another job applicant is, has been, or would be treated in a comparable situation based on their protected ground(s).[791] The ban on direct discrimination has traditionally been viewed as aiming at formal equality, ensuring that like cases are treated alike.[792] A paradigmatic example of direct algorithmic recruitment discrimination is an algorithm that explicitly uses protected grounds as decision-making criteria, for example, by disregarding all women's applications.[793]

Less favourable treatment based on protected grounds is, as a general rule, prohibited. The Non-Discrimination Directives do not explicitly outline exceptions to the prohibition of direct discrimination. However, they permit Member States to adopt limited, national-level exceptions.[794] For instance, Member States may allow different treatment based on a protected ground if the characteristic in question constitutes a genuine and determining occupational requirement, provided that the

790 See also section 6.2 below. Preventing discrimination based on an open-ended list of protected grounds is inherently more complex than managing risks under a closed list. Of the different systems of protected grounds (i.e. fully open, fully closed and hybrid), see (Gerards and Borgesius 2022).

791 See RED Art. 2(2)(a), EED Art. 2(2)(a), and GED Art. 2(1)(a). On what counts as less favourable treatment, see, e.g., case C-83/14 *Chez*, paras 64 and 69. Of direct discrimination in prior scholarship, see (Ellis and Watson 2012, 143–48; Fredman 2022, 250–80) and especially regarding algorithmic direct discrimination, see (Adams-Prassl, Binns, et al. 2023; Wachter et al. 2021; Gerards and Xenidis 2020, 67–70; Hacker 2018, 1165–66). For case law of the ECtHR regarding direct discrimination, see (Registry of the European Court of Human Rights 2025, 12–13).

792 (Wachter et al. 2020, 748; Ellis and Watson 2012, 142; Barnard and Hepple 2000, 562). Cf. *Marc de Vos* has argued that the prohibition of direct discrimination has also been increasingly interpreted in a way that brings it closer to substantive equality in practice (De Vos 2020, 66).

793 See also (Kelly-Lyth 2021, 905).

794 See, e.g., RED Art. 4, EED Art. 4 and GED Art. 14(2). The EED leaves room for more national exceptions on grounds of age (Art. 6) and for generally protecting the rights and freedoms of others (Art. 2(5)). While not an exception to the principle of equal treatment, positive actions could possibly be used to justify the use of some ARSs, see RED Art. 5, EED Art. 7 and GED Art. 3. See also (Martínez-Ramil 2022, 20).

objective is legitimate and the requirement proportionate.[795] Based on CJEU case law, for example, possession of particular physical capacities can qualify as a genuine and determining occupational requirement, entitling the setting of age limits for certain positions.[796] *Isabelle Chopin and Catharina Germaine's* comprehensive comparative study shows that this exception has been widely adopted in Member States.[797] Nevertheless, the overarching starting point is that less favourable treatment based on protected grounds is prohibited. Consequently, the prohibition of direct discrimination is stricter than the prohibition of indirect discrimination or the more general ban on discrimination in CFREU Article 21, which prohibits 'any discrimination' but appears to include broader justification possibilities than what the Directives allow for direct discrimination.[798]

The ban on direct discrimination does not effectively address all forms of algorithmic discrimination, as explored in prior scholarship and Publication III.[799] Proving direct discrimination has been deemed particularly challenging in opaque algorithmic systems, since job applicants must demonstrate that they have been treated less favourably because of their protected grounds.[800] In ARSs, the decision-making process (i.e., the treatment) may often remain in a 'black box'.[801] Even where the grounds for a decision are visible and comprehensible to humans, it is possible that the decision was made based on an apparently neutral factor (i.e., a proxy) rather

795 See RED Art. 4, EED Art. 4, and GED Art. 14(2). See, e.g., case C-258/15 *Salaberria Sorondo,* paras 32-50 and C-749/13 *Vital Perez,* paras 60-74.

796 Hence, in case C-258/15 *Salaberria Sorondo*, it was possible to set an age limit requiring job applicants for the post of police officers to be under 35 years of age. In C-229/08 *Wolf*, an age limit of 30 years was deemed a genuine and determining occupational requirement for intermediate career posts in the fire service. Instead, in C-416/13 *Vital Pérez*, an age limit of 30 years was not deemed to constitute a genuine and determining occupational requirement for the recruitment of police officers, for the purpose of safeguarding operational capacity and proper functioning of the local police.

797 (Chopin and Germaine 2023, 69–70).

798 (Publication III / Parviainen 2024, 452). Pursuant to CJEU case law, different treatment under CFREU Art. 21 may be justified if its aim is legally permitted and the treatment is proportionate to the aim pursued. See e.g., C-356/12, *Glatzel*, para 43 and C-406/15 *Milkova*, para 55.

799 (Gerards and Xenidis 2020, 67, 70–71; Hacker 2018, 1153; Xenidis and Senden 2020, 172; Martínez-Ramil 2022, 3; Wachter et al. 2021, 7; Rigotti and Fosch-Villaronga 2024, 15; Publication III / Parviainen 2024, 440). In prior research, the importance of indirect discrimination in tackling algorithmic discrimination has often been highlighted.

800 (Gerards and Xenidis 2020, 67, 70–71; Hacker 2018, 1153; Xenidis and Senden 2020, 172; Martínez-Ramil 2022, 3; Wachter et al. 2021, 13; Rigotti and Fosch-Villaronga 2024, 15; Publication III / Parviainen 2024, 440).

801 (Pasquale 2015, 3; Kim 2017, 921–22).

than on a protected ground.[802] However, if the neutral factor employed in decision-making is inseparably linked to a protected ground, the scenario could constitute proxy discrimination[803]. In prior scholarship, proxy discrimination has frequently been classified as indirect discrimination.[804]

Nonetheless, based on CJEU case law, I argued in Publication III that proxy discrimination could also meet the criteria for direct discrimination. This would be the case if the proxy used in the ARS is identifiable and understandable (e.g., a limit on years of work experience), inextricably linked to a protected ground (i.e., age in this case), and its use leads to unfavourable treatment of a protected group. If the proxies remain unintelligible or invisible, which might often be the case with complex ARSs, the CJEU case law may still provide a basis for establishing direct discrimination. Specifically, if a protected ground played a determinative role in the algorithmic recruitment process (e.g., by being reflected in the training data and thus influencing the decision-making rules[805]), and this caused less favourable treatment, such a situation might constitute direct discrimination. This second approach could, in principle, have broader applicability to intractable state-of-the-art ARSs, potentially constraining the use of opaque ARSs.[806] However, it remains largely speculative, relying mainly on the *Chez* judgment.[807] As a result, the likelihood of finding opaque ARSs directly discriminatory appears modest.[808] Nevertheless, since

802 See, e.g., (Cofone 2018, 1413; Gerards and Xenidis 2020, 72; Prince and Schwarcz 2020, 1281; Publication III / Parviainen 2024, 439).

803 (Weerts et al. 2024, 1851; Rigotti and Fosch-Villaronga 2024, 5; Gerards and Xenidis 2020, 72).

804 (Gerards and Xenidis 2020, 67, 70–71; Hacker 2018, 1153; Xenidis and Senden 2020, 172; Martínez-Ramil 2022, 3; Wachter et al. 2021, 20; Carter 2024, 358; Rigotti and Fosch-Villaronga 2024, 5). In practice, the line between direct and indirect discrimination is often blurred (Gerards and Xenidis 2020, 73).

805 See (Publication III / Parviainen 2024, 449–50). Since many LLMs are trained on data scraped from the public internet, protected grounds are likely embedded in the training data. See also (Solove and Hartzog 2024, 51).

806 Under this approach, if job applicants or their representatives successfully bring claims against employers, liability might arise solely from a lack of transparency, as direct discrimination permits few justifications.

807 See C-83/14 *Chez*, paras 76 and 91. For a more detailed discussion on this interpretative line, see (Publication III / Parviainen 2024, 448–50).

808 See, e.g., (Cofone 2018, 1413; Gerards and Xenidis 2020, 72; Prince and Schwarcz 2020, 1281; Publication III / Parviainen 2024, 439).

preventing ARSs from relying on proxies could be practically impossible, the risk of indirect discrimination exists.[809]

Indirect discrimination may occur in recruitment when an apparently neutral provision, criterion or practice puts job applicants with a specific protected ground at a particular disadvantage compared with other applicants.[810] For example, if an ARS that screens job applications prioritises recent graduates, it could particularly disadvantage older applicants with older degrees. In prior research, for instance, *Philipp Hacker* has suggested that, in algorithmic contexts, the algorithmic procedure itself could be considered a neutral practice that puts persons at a particular disadvantage.[811] However, the wording of the Non-Discrimination Directives could also support a more nuanced interpretation, in which the criteria or factors used by the ARS place certain applicants at a particular disadvantage.[812] As will be explained below, whether courts will treat ARSs as algorithmic procedures or require examination of the criteria or factors used by ARSs may affect the justifiability of the particular disadvantages that ARSs may create.

Namely, the prohibition of indirect discrimination contains an explicit exception: if the provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary, there is no indirect discrimination.[813] In contrast to direct discrimination, here the justification possibility derives directly from EU legislation and is open-ended, making it more broadly applicable.[814] To be justifiable, the provision, criterion or practice should fulfil all three elements of (1) legitimate aim, (2) appropriateness and (3) necessity.[815]

809 Incomprehensible or undetectable proxies may particularly disadvantage certain protected groups, thereby constituting prima facie indirect discrimination. However, applying the prohibition of indirect discrimination in algorithmic recruitment also faces specific challenges, and it is not straightforward either (Gerards and Xenidis 2020, 41–47).

810 Art. RED Art. 2(2)(b), EED Art. 2(2)(b), and GED Art. 2(1)(b). The ban on indirect discrimination aims at ensuring substantive equality, meaning equality of opportunity that cannot be achieved solely by disregarding protected grounds and treating everyone similarly, but rather requires active measures to address existing biases (Wachter et al. 2020, 749; Fredman 2016).

811 (Hacker 2018, 1161–62). See also (Kelly-Lyth 2023, 154; Martínez-Ramil 2022, 20–21; Adams-Prassl, Binns, et al. 2023, 151). Similarly, from the UK perspective, see (Kelly-Lyth 2021, 906).

812 See also (Kelly-Lyth 2023, 156–57).

813 RED Art. 2(2)(b), EED Art. 2(2)(b), and GED Art. 2(1)(b).

814 See also (Gerards and Xenidis 2020, 73; Kelly-Lyth 2023, 154).

815 The second and third criteria can be grouped into a 'proportionality' analysis, see, e.g., (Kelly-Lyth 2023, 155; Wachter et al. 2020, 751; Gerards and Xenidis 2020, 73). Cf. Hacker has viewed the proportionality analysis as a separate fourth criterion that necessitates an overall balancing of interests (Hacker 2018, 1163–65).

How the CJEU will interpret these elements of justification in the algorithmic recruitment context could significantly affect the practical reach of the indirect discrimination ban and, consequently, the extent to which ARSs are constrained. As an exception to a rule protecting fundamental rights, the justification possibilities should be interpreted narrowly.[816] Despite this, prior scholarship suggests that in many ARS use cases, employers may be able to justify the use of ARSs that, at first glance, appear to be indirectly discriminatory.[817]

First, prior studies suggest that there may be several legitimate aims justifying the use of the ARS, such as increasing the quality of recruitment decisions through greater consistency, reducing time to hire, enhancing the efficiency of the recruitment process, and allowing more applicants to be interviewed.[818] However, not all aims qualify as legitimate under the Non-Discrimination Directives, and courts must thoroughly analyse the legitimacy of the aims. For instance, cost savings alone should not constitute a legitimate aim,[819] but combined with other factors, such as the state of the employment market, those might suffice.[820] *Kelly-Lyth* has argued that the EU non-discrimination legislation aims to advance substantive equality,[821] which could lead courts to question the legitimacy of the aims of algorithmic systems that only maintain the existing unequal situation and do not seek to rectify the inequalities.[822] However, legitimate aims to use ARSs that advance substantive equality could also exist, for example, correcting human biases and prejudices that distort recruitment decisions.

Second, the means of achieving the legitimate aim must be appropriate.[823] The interpretation of appropriateness may vary depending on the level of scrutiny, i.e., whether it is the overall use of the ARS or a specific criterion employed by the system that is to be justified. In prior scholarship, appropriateness has often been linked to the effectiveness of the algorithmic system,[824] which can be

816 See, e.g., cases C-222/84 *Johnston*, para 36 and C-450/93 *Kalanke*, para 21.

817 (Martínez-Ramil 2022, 3). *Aislinn Kelly-Lyth* also appears to deem this possible under UK law, see (Kelly-Lyth 2021, 906–7). On justifiability of indirect algorithmic discrimination in general, see also (Hacker 2018, 1160 and 1164–65; Adams-Prassl, Binns, et al. 2023, 151–52).

818 (Kelly-Lyth 2021, 906; Martínez-Ramil 2022, 14; Hacker 2018, 1161).

819 See, e.g. joined cases *Schönheit* (C-4/02) and *Becker* (C-5/02), para 85.

820 See case C-127/92 *Enderby*, para 26. Moreover, mere generalisations are not enough to constitute legitimate aims, see case C-171/88 *Rinner-Kühn*, para 14.

821 See also (Wachter et al. 2020, 745).

822 (Kelly-Lyth 2023, 156).

823 Prior scholarship also refers to suitability in this regard, see also (Hacker 2018, 1161).

824 The effectiveness element has been noted by several scholars, see, e.g., (Gerards and Xenidis 2020, 73; Kelly-Lyth 2023, 155–57; Hacker 2018, 1161–62). *Philipp Hacker* has emphasised that the effectiveness of the algorithmic procedure is to be shown, and not the individual factors that led to the algorithmic output, see (Hacker 2018, 1161–62).

demonstrated, for instance, by showing the system's predictive accuracy.[825] In this context, predictive accuracy refers to the ARS's ability to generate predictions that correspond to actual outcomes, such as accurately reflecting applicants' job performance.[826] Alternatively, a more stringent interpretation would require the employer to demonstrate that the features identified and utilised by the algorithm are appropriate for achieving the legitimate aim.[827] For instance, if the legitimate aim is to predict applicants' work performance more accurately and objectively, the employer should be able to show that the features utilised serve that purpose.[828] If the more stringent interpretation is applied, it could be practically impossible to justify opaque ARSs where the features used remain unknown or undecipherable to humans.[829]

Third, for the means to be justifiable, they must also be necessary to achieve the legitimate aim. Necessity is generally understood as the absence of less discriminatory means to achieve the same result.[830] The benchmark against which the ARS is evaluated can be a human decision-making process or another algorithmic system.[831] Allegedly, the necessity of an ARS might be demonstrated, for example, by showing the biases and inefficiencies of human decision-making and the bias-mitigation measures implemented during the ARS's development.[832] However, if less biased training datasets were available, or if a less discriminatory algorithm could have been employed at equivalent cost, using a more biased alternative would not be justifiable.[833] Therefore, the ARS, or a specific criterion it

825 *Philipp Hacker* appears to deem predictive accuracy an important factor in demonstrating appropriateness (Hacker 2018, 1162–63). For criticism of the predictive accuracy criterion, see (Kelly-Lyth 2023, 155–57).

826 See also (Hacker 2018, 1150). While it is possible to evaluate the job performance of the selected applicants, information on the rejected applicants' performance remains unavailable.

827 Of this interpretation, see, e.g., (Kelly-Lyth 2023, 156; Hacker 2018, 1161). From the US perspective, see also (Grimmelmann and Westreich 2017, 173–74).

828 *Pauline Kim* has argued that showing a statistical correlation should not suffice as a justification, see (Kim 2017, 921–22).

829 See also (Hacker 2018, 1161).

830 C-83/14 *Chez*, paras 120 and 121. See also (Hacker 2018, 1162; Wachter et al. 2020, 775; Martínez-Ramil 2022, 13).

831 Of the comparison between a human and an algorithmic system, see, e.g., (Kelly-Lyth 2023, 157–59).

832 (Hacker 2018, 1162–63). See also (Kelly-Lyth 2023, 157–59).

833 (Hacker 2018, 1162–63; Martínez-Ramil 2022, 19). Consequently, while it is the employer that has to prove the justifiability of ARS use, the decisions made in the development phase can significantly affect the employer's justification possibilities.

applies, can only be deemed necessary if no other less discriminatory options were available to achieve the same aim.[834]

To sum up, ARSs that disadvantage certain groups of job applicants may be exceptionally justified if the use of the ARS or the criteria it employs are appropriate, for example, for making the recruitment processes more consistent, effective and generally more inclusive and if no other as effective and less discriminatory alternatives exist. However, the CJEU has not yet decided on an algorithmic discrimination case in the employment context and it remains to be seen which approach it will take. If interpreted leniently and focusing on the ARS-level, their potential particularly disadvantaging effects could be more easily justified, which would considerably weaken the force of the indirect discrimination ban and job applicants' protection. Instead, turning the gaze to the justifiability of the factors ARSs rely on could make it difficult to justify the use of opaque state-of-the-art ARS where those factors remain inscrutable. The latter approach could impose considerable practical constraints on the use of opaque ARSs.[835]

While the employers' primary objective should be to employ systems that are neither directly nor indirectly discriminatory, employers should carefully consider the justification possibilities even before deployment.[836] Evaluating the legitimate aim, appropriateness and necessity of the ARS in advance can help employers ensure that they can reasonably justify the use of that specific ARS in the event of potential legal challenges. Such ex-ante assessments could also be sound from a business perspective, as such assessments could reduce the likelihood of adopting systems that are unnecessary or poorly suited to the intended purpose.[837] Beyond initial assessments, continuous monitoring of ARSs' performance throughout their lifecycle is essential to identify potential discriminatory outcomes and implement corrective measures promptly.

As regards sanctions for discriminatory ARSs, Member States have the freedom to determine the sanctions to be imposed, provided they are effective, dissuasive and proportionate.[838] When compared with data protection or market surveillance

834 For instance, *Pablo Martínez-Ramil* has argued that algorithmic recruitment could lead to unjustifiable indirect discrimination in cases where poor design choices are made, such as using biased or incomplete datasets, and where less discriminatory alternatives are available (Martínez-Ramil 2022, 21).

835 See also section 6.2 below.

836 See also (Wachter et al. 2020, 775).

837 These assessments could, for instance, be included in a data protection impact assessment.

838 See RED Art. 15, EED Art. 17 and GED Art. 18.

authorities, the equality bodies' powers[839] are more limited, including conducting inquiries[840], providing non-binding opinions or binding decisions[841] and acting in court proceedings[842]. Unlike in cases of significant breaches of the GDPR and the AIA, the equality bodies do not have an explicit right to prevent the employer from using a discriminatory ARS under the Non-Discrimination and Standardisation Directives.[843]

In addition to the bans on discrimination, the GDPR Article 9 ban on processing special categories of personal data also applies to all ARSs. The special categories of personal data, which are 'by their nature, particularly sensitive in relation to fundamental rights and freedoms', are exhaustively listed in GDPR Article 9.[844] These categories partly resemble, partly diverge from the protected grounds listed in the Non-Discrimination Directives. According to the GDPR, special category data refers to data revealing racial or ethnic origin*, political opinions*, religious or philosophical beliefs, *trade union membership*, *data concerning health, sex life*, or sexual orientation, and the *processing of genetic data or biometric data to uniquely identify a natural person*. Compared to the Non-Discrimination Directives, age and gender are not included in the list; however, it does cover several items (marked in italics above) that the Non-Discrimination Directives do not protect. Yet determining

839 The Equality Bodies' Powers are to be standardised and enhanced based on the two Directives on Standards for Equality Bodies adopted in May 2024. See Council Directive (EU) 2024/1499 of 7 May 2024 on standards for equality bodies in the field of equal treatment between persons irrespective of their racial or ethnic origin, equal treatment in matters of employment and occupation between persons irrespective of their religion or belief, disability, age or sexual orientation, equal treatment between women and men in matters of social security and in the access to and supply of goods and services, and amending Directives 2000/43/EC and 2004/113/EC and Directive (EU) 2024/1500 of the European Parliament and of the Council of 14 May 2024 on standards for equality bodies in the field of equal treatment and equal opportunities between women and men in matters of employment and occupation, and amending Directives 2006/54/EC and 2010/41/EU (hereinafter 'the Standardisation Directives').

840 Art. 8 of the Standardisation Directives.

841 Art. 9 of the Standardisation Directives.

842 Art. 10 of the Standardisation Directives leaves room for Member States to determine what kinds of actions are allowed for Equality Bodies.

843 However, based on Art. 9 of the Standardisation Directives, the equality bodies may be empowered in Member State legislation to issue binding decisions, including specific measures to prevent further occurrences of discrimination, which could also comprise ceasing the use of a discriminatory ARS. For instance, in Finland, the occupational safety and health authorities may oblige an employer to remedy or eliminate non-complying conditions within a specified time limit and set a default fine to strengthen the obligation, see Section 15 of the Act on Occupational Safety and Health Enforcement and Cooperation on Occupational Safety and Health at Workplaces (44/2006).

844 GDPR Recital 51.

where the data processed constitutes special category personal data may be challenging, as 'normal' personal data might reveal such data through inference.[845] Nevertheless, unlike the bans on discrimination, the applicability of the ban on processing special category personal data is not dependent on any comparisons, or analysis or proof of the effects of the processing on job applicants.[846]

However, GDPR Article 9 contains several exceptions under which the processing of special category data may be permitted. Three of the exceptions (GDPR Article 9(2)(a), (b) and (e)) initially appear relevant for ARSs, but at times, other exceptions may also apply.[847]

First in order is job applicants' explicit consent to the processing of their special category personal data, which is highly unlikely to be applicable.[848] According to the EDPB, explicit consent must be given as an express statement, such as a signed written statement or by completing an electronic form.[849] In order to be valid, the consent should also meet the general criteria established in GDPR Article 4, point 11 of being 'freely given, specific, informed and unambiguous indication of the data subject's wishes'.[850] Due to the power imbalance between job applicants and employers, and the feared or actual risk of adverse effects arising from a refusal, the EDPB has considered it unlikely that job applicants' consents would be freely given.[851] This is not the only problem, as for consent to be specific and informed enough, the job applicant should know precisely which special category data will be processed in the ARS, which can be difficult to ascertain in opaque ARSs that may

845 See, e.g., C-21/23 *Lindenapotheke*, paras 82-83 and 88; C-184/20 *Vyriausioji tarnybinės etikos komisija*, paras 123 and 127. See also (Wachter and Mittelstadt 2019, 564; Zarsky 2017, 1013). Another contradictory question is whether and when inferred data is considered personal data under the GDPR and what data subjects' rights apply to inferred data, see, e.g., (Wachter and Mittelstadt 2019, 498) and C-434/16 *Nowak*.

846 Of the required proof in cases claiming breach of this prohibition, see section 6.1.1.2 below.

847 The necessity for occupational medicine and for the assessment of the working capacity of the employee might also apply in certain instances, where the work poses specific requirements on health (Art. 9(2)(h)). Applicable could also be the exception of necessity for reasons of public interest in the area of public health (Art. 9(2)(i)), if Member State law would allow processing of particular vaccination data to prevent certain diseases from spreading across the borders. See also (Publication I / Viljanen and Parviainen 2022, 3).

848 GDPR Art. 9(2)(a).

849 (EDPB 2020c, 20–21).

850 See GDPR Recitals 32, 42 and 43 and (EDPB 2020c, 9).

851 (EDPB 2020c, 9). Similarly, concerning the employment context, also in (WP29 2017b, 3–4; 6–7; Otto 2018, 400; Abraha 2023, 184; Warter 2025, 181). However, the circumstances of each recruitment process must be considered. While it is a strong assumption that applicants' consents are not freely given, there could also be more balanced situations, see also (Publication II /Parviainen 2022, 243–44).

infer special category data even without the employer's awareness.[852] Furthermore, even when the consent is exceptionally valid, it may be revoked at any time.[853]

The second potential exception is GDPR Article 9(2)(b), which permits processing of special category personal data where necessary for carrying out the obligations and exercising specific rights under employment law. In the algorithmic recruitment context, this could cover, for instance, disability-related information required to assess reasonable accommodation needs.[854] However, such legal obligations are more likely to exist during an employment relationship than during the recruitment process.

GDPR Article 9(2)(e) offers a third potential basis for processing special category personal data, where the job applicants have made the personal data manifestly public. For instance, where a job applicant has made their political opinions public on their professional social media profile, ARSs may be allowed to process this data if it is necessary to fill the position.[855] Nevertheless, the scope of this exception turns heavily on both the meaning of 'manifestly public'[856] and the necessity requirement, neither of which is straightforwardly satisfied.

Taken together, these exceptions show that processing of special category personal data in algorithmic recruitment is not categorically prohibited. Nevertheless, at the moment, no single exception provides a legal basis for such processing across the recruitment context as a whole. Each exception has its specific conditions, the applicability of which must be assessed on a case-by-case basis.

Furthermore, if the ARS makes automated decisions, the use of special category personal data is even more constrained by GDPR Article 22(4) and is permitted only on the basis of explicit consent or substantial public interest.[857] While the substantial public interest exception could apply in the development phase,[858] where special

852 Of the requirements of specific and informed, see also (EDPB 2020c, 13–17).

853 GDPR Arts. 9(2)(a) and 7. See also (EDPB 2020c, 9; Publication II /Parviainen 2022, 242–45; Abraha 2023, 184; Warter 2025, 181).

854 GDPR Art. 9(2)(b) and EED Art. 5.

855 GDPR Art. 9(2)(e). See case C-446/21 *Schrems v. Meta*, paras 80–83 on the extent of this derogation. See GDPR Art. 5(1)(c). Of the processing of personal data from social media profiles during recruitment in general, see (WP29 2017b, 11).

856 See C-252/21 *Meta Platforms and Others,* para 77, where it is stated that this requires intention to 'explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public'.

857 GDPR Art. 22(4).

858 AIA Art. 10(5) also contains an exception under which processing of special category data is exceptionally allowed for ARS providers, if it is 'strictly necessary for the purpose of ensuring bias detection and correction' in the ARSs and there are appropriate safeguards for fundamental rights in place. The AIA Art. 10(5) lists several conditions which must be met for the processing to be lawful. However, this provision applies only to providers.

category data may be needed to make ARSs non-discriminatory, it is less likely to apply in the use phase when automated decisions are made.[859] Given the above-discussed obstacles to job applicants' consent, ADM based on special category personal data in recruitment appears to be mostly prohibited.

All in all, complying with the ban on processing special category personal data is difficult in practice. Employers should ensure that an ARS does not process special category personal data unless at least one of the exceptions applies. While employers could prevent their personnel and job applicants from entering explicit special category personal data into the ARS,[860] ensuring that such data is not inferred from 'normal' personal data is already a significantly greater challenge. To complicate matters further, if the ARS is based on an AI model that contains personal data, the EDPB appears to require that controllers who deploy such AI models conduct due diligence to verify that the model was not developed by unlawfully processing personal data.[861] It is unclear, however, whether this requirement applies to AI system providers that integrate an AI model into a broader system, or to the end deployer of that system.[862] If employers deploying ARSs are subject to this requirement, compliance could be highly burdensome: independently verifying whether an ARS was trained on special category data, or whether that training was otherwise lawful, may be practically infeasible. A more workable approach for employers may be to obtain contractual guarantees from vendors that the ARS relies on anonymous AI models, thereby removing the need to verify the lawfulness of data processing during the model's development. Nevertheless, this would not remove the obligation to ensure that during deployment, the ARS processes special category data only when a GDPR Article 9 exception applies.

GDPR Article 10 could also be interpreted as a qualified ban on the processing of personal data relating to *criminal convictions and offences or related security*

859 On the need to utilise special category data to make the algorithmic systems non-discriminatory, see also (Žliobaitė and Custers 2016, 185 and 198; van Bekkum and Zuiderveen Borgesius 2022, 3).

860 The employers should educate their staff on this requirement and provide them with guidance. Similarly, job applicants could be guided and warned against including sensitive data in their applications. See also (Barberá 2025, 29). Nevertheless, there is a considerable risk that employees will not follow the guidelines and policies, highlighting the importance of monitoring. *Nicole Gillespie et al.* found in a global study that almost half of employees admitted to using AI in ways that contravened organisational policies and guidelines (Gillespie et al. 2025, 75).

861 (EDPB 2024b, 34). Although the EDPB Opinion does not specifically discuss special category data, the general level requirement to ascertain the lawful development of the model could also apply to the unlawful processing of such data.

862 (EDPB 2024b). Herein, it is read to extend to the deployers of the AI system as well, although this could create practically very challenging obligations.

measures[863] in algorithmic recruitment, as it demands that such processing may be carried out only under the control of official authority or when it is authorised by EU or Member State law that provides for appropriate safeguards.[864] There is no such EU legislation that would allow the processing of such personal data in recruitment. Accordingly, at the EU level, this qualified ban appears to be rather strict, basically prohibiting the processing of criminal conviction and offence data in ARSs.

However, the strictness of the qualified ban on processing criminal conviction and offence data ultimately depends on the Member State legislation. For instance, in Finland, the processing of criminal conviction and offence data is required for job applicants chosen for a position that, on a permanent basis and to a material degree, includes raising, teaching, caring for, or looking after a minor, or other work performed in personal contact with a minor.[865] Nevertheless, given the requirement to ensure appropriate safeguards for the rights and freedoms of data subjects under Member State law, the situations in which processing of criminal conviction and offence data is permitted should be limited.

There is no similar limitation to making automated decisions based on criminal conviction or offence data, as there is regarding special category personal data.[866] Thus, if Member State law allows the processing of criminal conviction and offence data, it appears possible to also base automated decisions on that data, if the other criteria for such decision-making are met.[867] Nonetheless, for instance, in Finland, there would be no need for automated decisions, as criminal conviction and offence data may be processed only for the selected applicants.

Compared with bans on discrimination, the GDPR's bans on processing special category data and processing of personal data relating to criminal convictions are more severely sanctioned at the EU level, and data protection authorities have wider

863 The GDPR does not define what is meant by criminal convictions, offences, or related security measures. In case C-136/17 *GC and Others v CNIL*, para 72 it was confirmed that 'information concerning legal proceedings brought against an individual, such as information relating to the judicial investigation and the trial, [… and] the ensuing conviction is data relating to 'offences' and 'criminal convictions' […] regardless of whether or not […] the offence […] was shown to have been committed'. This suggests that data regarding suspicion or allegations of criminal activity could also be covered. Of such an approach in the UK, see (ICO 2021). 'Security measures' would, according to *Ludmila Georgieva,* cover measures concerning criminal offences such as revocation of a driver's licence (Georgieva 2020, 388–89).

864 GDPR Art. 10 refers to Art. 6(1) on the lawful basis of processing, see section 5.2.2 below for a more detailed discussion on it.

865 Act on Checking the Criminal Background of Persons Working with Children (504/2002), particularly Sections 2 and 3. See also Security Clearance Act (726/2014).

866 See GDPR Art. 22(4).

867 See below for the qualified prohibition on ADM.

powers.[868] The data protection authorities can, for example, issue warnings and reprimands, orders to comply, impose limitations (including bans) on processing and impose administrative fines.[869] The administrative fine could be up to 20 million euros or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[870] For instance, the Hamburg DPA has fined H&M 35.3 million euros for data protection violations related to the processing of employees' data, including health-related information.[871]

Qualified ban on two AI practices

The AIA includes two categories of AI practices subject to qualified bans that are relevant in algorithmic recruitment. The first ban concerns the inference of emotions in the workplace and does not apply if the AI system is used for medical or safety reasons (AIA Article 5(1)(f)).[872] The ban could be interpreted literally and narrowly, to cover only the physical workplace and the duration of the employment relationship.[873] However, a broader teleological interpretation, extending to telework and recruitment, would more effectively align with the ban's and the AIA's fundamental rights-protecting purpose.[874] The concept of inferring emotions should also be interpreted broadly, in line with AIA Article 3, point 39, to include both the

868 GDPR Art. 10 is not explicitly mentioned in Art. 83 as giving rise to a fine, but processing personal data relating to criminal convictions and offences would breach at least Art. 5(1)(a) and likely also Art. 6(1), and hence give rise to similar fines as breach of the Art. 9.

869 GDPR Art. 58(3).

870 GDPR Art. 83(5)(a). For potential remedies available to job applicants, see section 6.1.1.2 below.

871 (EDPB 2020d).

872 For the interpretation of the exceptions, see also (European Commission 2025c, 87–88).

873 Of the narrow interpretation, see also (Cristofolini 2024, 83).

874 In Annex III, point 4, access to employment is covered under the title 'employment, workers management and access to self-employment', which would hint that the recruitment phase is understood as part of the workplace broadly understood. In support of a broader reading, see also (Cristofolini 2024, 83; EDPS 2024, 7; European Commission 2025c, 85). Of the rationale of the ban, see AIA Recital 44.

identification[875] and inference[876] of emotions and intentions.[877] For instance, AI systems that infer job applicants' emotions during video interviews based on their movements and gestures would be banned under AIA Article 5(1)(f).

Although qualified, the ban is, in practice, nearly absolute in recruitment, as medical or safety justifications for emotion inference are difficult to conceive in this context. Nevertheless, the ban has a narrow scope, applying only to specific ARSs that employ emotion-inference techniques, such as some video-interviewing systems. For example, it does not cover inferring emotions from data other than biometric data (e.g., written text).[878] Moreover, systems that merely infer physical states (e.g., sickness) without inferring emotions are not prohibited under AIA Article 5(1)(f).[879]

Further, the ban on crime-prediction AI systems under AIA Article 5(1)(d) might also be relevant in algorithmic recruitment. Namely, it is technically possible to use ARSs to assess or predict the likelihood that a job applicant will commit a criminal offence, based solely on profiling or the assessment of their personality traits and characteristics. The ban includes an exception, allowing the use of such systems where they only support human assessment of a person's involvement in a criminal activity and where the assessment is based on objective, verifiable facts linked to the criminal activity.[880] The wording of the AIA Article 5(1)(d) does not explicitly restrict this prohibition to the law enforcement domain.[881] Nevertheless, the Commission's guidelines suggest that such a limitation was intended.[882] Consequently, the relevance of this qualified ban is likely to remain modest in this context.

875 This refers to processing biometric data, such as facial expressions, to directly compare them with preprogrammed emotions to identify an individual's emotion (European Commission 2025c, 82).

876 Inference means deducing information generated by the system's processes, not only based on data collected about the natural person. For instance, ML-based emotion detection would be inference (European Commission 2025c, 82).

877 While the prohibition of AIA Art. 5(1)(f) utilises differing wording from that of AIA Art. 3, point 39, defining emotion recognition systems, the Commission guides that those should be read to have a similar scope (European Commission 2025c, 82).

878 (European Commission 2025c, 84).

879 AIA recital 18. See also (European Commission 2025c, 83). Nevertheless, such systems could be problematic from the point of view of data protection and GDPR Arts. 9 and 22(4).

880 This exception might apply, for instance, if information about a judgment in a criminal case is publicly available and a human recruiter uses information in that judgment to support the assessment.

881 See also (Kindt and Jasserand 2024, 125).

882 See (European Commission 2025c, 71–72). GDPR Art. 10 could also restrict such systems, provided that Member State law does not allow such processing.

Qualified ban on ADM

Finally, GDPR Article 22 *bans automated decision-making*.[883] Although worded as 'the right not to be subject to a decision based solely on automated processing', the CJEU confirmed in the *Schufa* case that the provision actually is a prohibition of ADM, which the individuals subject to the decision do not have to invoke.[884]

Briefly put, prohibited ADM takes place when (i) a decision is made,[885] (ii) the decision is based solely on automated processing (i.e. where humans are not meaningfully involved and do not affect the outcome)[886], and (iii) it has legal or similarly significant effects on the data subject.[887] The CJEU suggested in the *Schufa* case that these three criteria could be fulfilled at different stages of the decision-making process.[888]

According to the CJEU, the decision criterion is to be interpreted broadly.[889] Hence, it appears that intermediate or preliminary decisions, such as screening decisions or scores generated by ARSs, could also constitute ADM if a human recruiter strongly draws on them to refuse an applicant a job opportunity or to pass them on in the recruitment process.[890] Such intermediate or preliminary decisions may also have legal or similarly significant effects on job applicants.[891] Yet it is unclear when the decision is 'solely automated' and what kind of human involvement would take the processing outside the scope of the ADM ban. In the *Schufa* case, the CJEU confirms that ADM could take place where a human 'draws strongly on' an automatically generated probability value.[892] This stance rules out a narrow literal interpretation, where any human intervention drops the ARS out of the

883 For what counts as ADM, see (Publication II /Parviainen 2022, 234–40) and sections 2.3 and 4.2 above.

884 C-634/21 *Schufa*, para 52. For discussion on this point, prior to the Schufa judgment, see (Publication II /Parviainen 2022, 229–34).

885 See also Case C-634/21 *Schufa*, paras 44–46 and AG Pikamäe's Opinion para 43.

886 See also Case C-634/21 *Schufa*, para 62 and AG Pikamäe's Opinion in paras 36, 43–47 and (Aza 2024, 17).

887 (Publication II /Parviainen 2022, 236–37; Bygrave 2020, 532; Brkan 2019a, 99) and C-634/21 *Schufa* para 43.

888 See Case C-634/21 *Schufa*, paras 43, 48 and 73. See also (Aza 2024, 13 and 17). Cf. (Publication II /Parviainen 2022, 239).

889 See C-634/21 *Schufa*, paras 44–46.

890 (Publication II /Parviainen 2022, 237). See also C-634/21, para 62 and AG Pikamäe Opinion in Schufa, paras 34–35 and 43–47. Pikamäe emphasised that the effects should have a serious impact, comprising, for instance, legal effects and economic consequences. The recruitment decisions are likely to have both types of effects.

891 (Publication II /Parviainen 2022, 237).

892 See C-634/21 *Schufa*, para 73.

ADM ban's scope.[893] Nevertheless, the judgment does not elaborate on what the 'draws strongly on' threshold means in practice. Instead, the WP29 guidelines on ADM and profiling are more informative in this regard as they state that as human involvement qualifies only 'oversight of the decisions [which] is meaningful, rather than just a token gesture', it should be carried out by someone who has the authority and competence to change the decision and include consideration of all the relevant data.[894] Nonetheless, the guidelines are not binding, and it remains somewhat unclear what kind of processing ultimately qualifies as prohibited ADM, and how often ARSs actually involve ADM.[895]

In any case, the ban is not absolute.[896] GDPR Article 22(2) allows ADM if it is (a) necessary for entering into or performing a contract, (b) authorised in legislation which offers suitable safeguards, or (c) explicitly consented to by the data subject.[897] To my knowledge, there is no EU-level legislation that would authorise the use of ADM in recruitment.[898] Given that job applicants' consents are seldom freely given or informed,[899] the necessity for entering into a contract could be the most viable exception under which ADM might be allowed.[900] The WP29 guidelines on ADM and profiling also cite job application screening as an example of necessary ADM to enter into a contract, though in that example, there were tens of thousands of applications.[901]

893 Of such an interpretation, see, e.g., (Wachter et al. 2017, 88 and 92). See also (Zarsky 2017, 1018). Under the narrow interpretation, for instance, implementation of the AIA's human oversight measures could mean that there is no ADM. See AIA Art. 14 and 26(2).

894 (WP29 2018a, 21). As an example of fabricated human involvement, the WP29 cites the routine application of automatically generated profiles to individuals without any actual influence on the outcomes. Of the broader interpretation, where decisions are deemed to be made based on 'solely automated processing' if humans are only nominally involved, see also (Mendoza and Bygrave 2017, 11; Bygrave 2020, 532–33; Kamarinou et al. 2016, 11–12; Sartor and Lagioia 2020, 59–60; Publication II /Parviainen 2022, 236).

895 Some scholars have deemed that ADM is rare in the recruitment context (Carter 2024, 351–52), while others have found, for instance, that many recruitment agencies utilise ADM in their recruitment work (Larsson et al. 2024, 9).

896 See also (Publication II /Parviainen 2022, 240–42) and section 4.2.

897 See also C-634/21 *Schufa*, para 53.

898 A comparative study of Member States' laws is beyond the scope of this dissertation, see section 1.3.1 and 1.3.3. However, I did not encounter any national laws permitting ADM in recruitment in the course of this study.

899 (EDPB 2020c, 9 and 19–20). Similarly, concerning the employment context, also in (WP29 2017b, 3–4; 6–7; Otto 2018, 400; Abraha 2023, 184; Warter 2025, 181).

900 (Publication II /Parviainen 2022, 240–42).

901 (WP29 2018a, 23).

Nevertheless, ADM is not always necessary for entering into an employment contract. Based on CJEU case law, the necessity requirement must be interpreted strictly, meaning that mere practicality, usefulness or administrative convenience of ADM is insufficient.[902] Employers must also consider whether alternative, less intrusive means could achieve the same purpose.[903] For instance, *Kelly-Lyth* has argued that the necessity of a solely automated hiring system, compared to scores reviewed by a human recruiter, could be difficult to demonstrate.[904] Since multiple factors may affect the necessity of the ADM, the applicability of the contractual necessity exception should be assessed on a case-by-case basis for each position to be filled.[905] In Publication II, I argued that under the contractual necessity exception, ADM could be permitted, for instance, if it would be practically impossible or unreasonable to process the applications by other, less privacy- and rights-intrusive means. When assessing the situation, the employer's circumstances and the specific recruitment context should be noted, such as the size of the employer, its financial resources and number of personnel, the number of applications expected for the open position and the total number of applications received per year.[906] If ADM is not necessary to enter into an employment contract, it is likely banned, given the legal and practical hurdles job applicants' consents face.[907]

Yet, the general requirements of consent appear more problematic than the requirement of explicitness demanded by GDPR Article 22(2)(a). The EDPB has considered that, to be explicit, the data subject should 'give an express statement of consent', for instance, by filling in an electronic form, using an electronic signature, or using two-stage verification, which does not pose an undue burden in the algorithmic recruitment context.[908] However, job applicants' consents are unlikely to meet the criteria required by GDPR Article 4, point 11 of being 'freely given, specific, informed

902 See, e.g., CJEU cases C-73/07 *Satakunnan Markkinapörssi Oy and Satamedia Oy*, para 56, C-92/09 and 93/09 *Volker und Markus Schecke and Eifert*, paras 77 and 86, C-473/12 *IPI*, para 39, C-293/12 *Digital Rights Ireland*, para 52, C-212/13 *Ryneš*, para 28 and C-13/16 *Rīgas satiksme*, para 30.

903 (WP29 2018a, 23).

904 (Kelly-Lyth 2021, 917).

905 See also (Publication II /Parviainen 2022, 240–42). The contractual necessity exception could apply, for instance, more often in the screening phase of mass-scale recruitment scenarios than in situations where there are only a few applications. Likewise, sourcing applicants might have to be automated also in specialist recruitments, as there might be only a few suitable candidates, finding of which could be difficult.

906 See also (Publication II /Parviainen 2022, 240–42) and section 4.2.

906 (Publication I / Viljanen and Parviainen 2022).

907 Of the legal and behavioural problems related to consents under the GDPR in general, see, e.g., (Hacker et al. 2022, 73).

908 (EDPB 2020c, 20–22).

and unambiguous indication of the data subject's wishes'.[909] First, as mentioned above in relation to consents to processing special category data, given the power imbalance and the feared or actual risk of adverse effects resulting from a refusal, the EDPB has deemed it unlikely that job applicants' consent would be freely given.[910] Second, considering the opacity and complexity of the ARSs, consent to ADM may not be sufficiently specific or informed.[911] The WP29 emphasised the importance of understanding exactly what data subjects are consenting to, including the envisaged use and consequences of the processing.[912] As noted by the EDPB, understanding the consequences of consent requires controllers to provide accessible information to data subjects, which may be difficult given the complexity and opacity of the ARSs, and potentially requires more information when ADM is involved.[913] The informed nature of consent may also be undermined by consent fatigue, where job applicants are overwhelmed by questionnaires and privacy policies and consent to ADM without reading or understanding the information provided.[914] It is up to the employers to prove that the consent is valid.[915] Nevertheless, even an initially valid consent can be withdrawn at any time, preventing further ADM, and making consent an unpredictable basis for using ADM.[916]

Furthermore, it must be noted that if the ADM involves special categories of personal data, it is not sufficient that an applicable exemption under GDPR Article 22(2) exists, as the additional requirements of Article 22(4) must also be met. As discussed above, these are unlikely to be satisfied during the ARS use phase, so employers should ensure that no special category data is processed in ARSs that

909 See GDPR Recitals 32, 42 and 43 and (EDPB 2020c, 9).

910 (EDPB 2020c, 9). Similarly, concerning the employment context also in (WP29 2017b, 3–4; 6–7; Otto 2018, 400; Abraha 2023, 184; Warter 2025, 181). However, the circumstances of each recruitment process must be considered. While it is a strong assumption that applicants' consents are not freely given, there could also be more balanced situations, see also (Publication II /Parviainen 2022, 243–44).

911 See, e.g., (Kuner et al. 2017, 1; Publication II /Parviainen 2022, 243–44; Abraha 2023, 184).

912 (WP29 2018a, 12–13).

913 Of the varying levels of information required to ensure genuine understanding, see also (EDPB 2020c, 16).

914 See, e.g., (EDPB 2020c, 19–20; Nouwens et al. 2020, 1; Edwards and Veale 2017, 66).

915 GDPR Art. 7(1) and Recital 42. The EDPB appears to place the burden on addressing consent fatigue on controllers (EDPB 2020c, 19). The WP29 has proposed layered privacy notices as one way to deliver information 'efficiently and succinctly' to avoid information fatigue (WP29 2018c, 7).

916 GDPR Art. 7(3). Yet, as EDPB has stated, the processing operations that took place in accordance with the GDPR before the consent was withdrawn remain lawful (EDPB 2020c, 24).

make automated decisions. This is, however, a formidable task, as even ordinary personal data can reveal special category data through inferences.[917]

Considering the limited scope of the exceptions, it appears possible that in many instances the use of ADM in algorithmic recruitment could be banned by GDPR Article 22. From a compliance perspective, the ban on ADM, along with the related safeguards and obligations, is demanding. Determining whether ADM takes place and whether any exception permits its use is more context-dependent than, for instance, determining whether an ARS qualifies as an AI system. The legal grounds for employing ADM should be assessed separately for each new use case and job opening. While prior assessments may remain valid for similar positions, any relevant changes in circumstances (e.g., size of the applicant pool) should be noted.

The inherent complexity of the ban on ADM could incentivise employers to meaningfully involve humans in the recruitment processes, as it could reduce the need to assess the legality of ADM use. However, even when humans are involved, employers must regularly monitor that humans are genuinely participating in the decision-making process and are not simply relying on the ARS without critical oversight. If human involvement becomes only a 'token gesture'[918] and the human 'draws strongly on' automatically generated output,[919] the decision-making could effectively become automated. Yet, if it is difficult for employers to detect such situations of automation creep, it will be so for those aiming to enforce the prohibition.

Breaching the ban on ADM is subject to the same substantial sanctions and enforcement mechanisms as the prohibitions of processing special category data and criminal conviction data discussed above.[920]

5.2.2 Obligations

The category of obligations comprises general requirements imposed on ARSs or procedures that employers must ensure are met to safeguard data protection and prevent discrimination. The less stringent wording of obligations distinguishes them from bans and justifies their classification as a separate category. Due to their generality, many of the obligations apply to all types of ARSs and could profoundly constrain or shape ARS use.

Although the obligations within this framework are directed at employers, compliance may prove challenging if ARS providers fail to account for these

917 See, e.g., C-21/23 *Lindenapotheke*, paras 82–83 and 88; C-184/20 *Vyriausioji tarnybinės etikos komisija,* paras 123 and 127. See also (Wachter and Mittelstadt 2019, 564; Zarsky 2017, 1013; Kosinski et al. 2013).

918 (WP29 2018a, 21).

919 C-634/21 *Schufa,* para 62.

920 See GDPR Arts. 58(3) and 83(5)(b).

requirements during the development phase. Non-compliance with these obligations carries largely the same consequences as breaching the qualified bans.[921]

Obligations regarding all ARSs

The GDPR imposes many general obligations on all ARSs that process job applicants' personal data.[922] While ARSs are likely to process personal data, some may not, such as those used solely for drafting job advertisements or job descriptions. Since all recruitment processes eventually involve personal data processing, the GDPR obligations discussed below are not exclusive to ARS use. That said, certain characteristics of ARSs may complicate compliance and raise novel issues.[923] As the EDPB's ChatGPT Taskforce has noted, however, technical impossibility does not justify non-compliance with the GDPR.[924]

To begin with, for the use of ARS to be lawful, the employer must have a lawful ground for processing personal data in the system, as required by GDPR Article 6.[925] The employer must decide on which lawful ground(s) it relies before the ARS is

921 See GDPR Arts. 58(3) and 83(5) as well as Arts. 8–10 of the Standardisation Directives. Breaching some of the provisions of the AIA discussed in this section should not trigger separate sanctions for the deployers; rather, those breaches could contribute to the finding of GDPR breaches and affect the sanctions under the GDPR.

922 GDPR Art. 4, point 1, defines personal data as 'any information relating to an identified or identifiable natural person'. It further clarifies that an identifiable natural person is 'one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. Of the broad interpretation of personal data, see, e.g., cases C-579/21 *Pankki S*, para 45 and C-604/22 *IAB Europe v. Gegevensbeschermingsautoriteit*, paras 32–51. See also (Purtova 2018).

923 See, e.g., (Drouard et al. 2024b). It appears to be demanding even for the regulators, such as the EDPB and national data protection authorities, to agree on how the central data protection requirements should be interpreted and implemented in the context of AI, especially generative AI. While the EDPB has published a few papers on generative AI, numerous open questions remain. See (EDPB 2024b; 2024c). Of nationally divergent prior opinions, see, e.g., (Hamburg Commissioner for Data protection and freedom of information 2024; Datatilsynet 2023).

924 (EDPB 2024c, 5).

925 GDPR Art. 6 lays down in this regard the legitimate basis as required in CFREU Art. 8. See C-496/17 *Deutsche Post*, para 57. See also C-252/21 *Meta Platforms and Others*, para 90, stating that GDPR Art. 6(1) sets out an exhaustive and restrictive list of cases where personal data processing can be deemed lawful.

used, and it must also communicate those to job applicants.[926] Typically, employers have the required information to determine the lawful grounds for processing, so this obligation does not impose an undue burden even when utilising some intractable ARSs. Yet, it is not certain that a lawful ground for processing personal data in ARSs always exists.

When using ARSs, four lawful grounds for processing are conceivable: necessity for entering into a contract at the job applicants' request[927], necessity for the legitimate interests of the employer or a third party which are not overridden by job applicants' fundamental rights and interests,[928] necessity for complying with an employer's legal obligation,[929] and, in certain exceptional cases, job applicants' consent.[930] Thus, the lawful grounds for processing personal data when using ARS for recruitment purposes do not significantly differ from those on which employers rely in traditional, human-conducted recruitment processes.

That said, the central question for each of the viable legal bases, excluding the seldom-applicable consent, is whether the processing is *necessary*, a requirement that warrants careful examination when applied to ARSs.[931] The necessity concept

926 GDPR Art. 5(2) and 13(1)(c). See C-252/21 *Meta Platforms and Others*, para 95. See also (EDPB 2024a, 4 and 6; Kotschy 2020a, 329). No single lawful ground has to cover all processing of personal data in the ARS. Rather, there may be simultaneously several lawful grounds that apply to different processing operations and purposes within the ARSs. As the EDPB has highlighted, the controller must clearly state 'which purpose applies to each element of data and which lawful basis is being relied upon'. See (EDPB 2020c, 24).

927 GDPR Art. 6(1)(b). Submitting a job application could be considered a request by the job applicant. Yet if the ARS is used in headhunting, there would likely be no job applicants' requests at the outset, making this basis inapplicable. See also (EDPB 2019a, 13; Kelly-Lyth 2021, 910).

928 GDPR Art. 6(1)(f) and Recital 47. In prior research, for instance, *Kelly-Lyth* has acknowledged this as a potential lawful basis for hiring algorithms (Kelly-Lyth 2021, 910).

929 GDPR Art. 6(1)(c). An employer's legal obligations may require that it process certain personal data, such as work and residence permits or vaccination status. For examples of such legal obligations in the Finnish context, see (Publication I / Viljanen and Parviainen 2022, 3).

930 GDPR Art. 6(1)(a) and Recital 43. Consent could be the legal basis, for instance, to add the job applicant's profile to an applicant pool, from which the employer may directly seek applicants for further openings in the near future. See also the EDPB FAQ on consent, where further storage of CVs has been considered possible under consent (EDPB 2026). However, the problems of job applicants' consents discussed above and in Publication II must be noted, see (Publication II /Parviainen 2022, 243–45) and (EDPB 2020c, 8–9; Abraha 2023, 184; Warter 2025, 181).

931 See GDPR Arts. 6(1)(b), (c) and (f). GDPR Recital 39 states that 'personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means'.

has an independent meaning in EU law, and its interpretation must fully reflect the objectives of data protection law.[932] The CJEU has interpreted the necessity requirement strictly,[933] since derogations and limitations to the protection of personal data must apply only insofar as is strictly necessary.[934] Based on CJEU case law, the necessity condition demands that 'the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects'.[935] Data protection authorities have adopted a similar strict interpretation, and based on EDPB guidance, merely useful processing that is not objectively necessary for the stated objectives would not count as necessary.[936] If there are other equally effective but less fundamental-rights-infringing alternatives available, the processing by ARSs may not be necessary for recruiting new employees.[937]

The strict necessity requirement could limit the situations where a lawful basis for processing personal data in the ARS exists. Human recruiters have conducted recruitment for years, so it is not self-evident that using ARSs is necessary.[938] For instance, although an employer's legal obligations may require it to process certain personal data, such as work and residence permits,[939] it is unlikely that there would be a legal obligation to utilise ARSs for such mandatory processing of personal data. Equally, the WP29 has considered that shorter decision-making processes, or their greater consistency, fairness or improved efficiency alone are not sufficient to show that profiling or ADM are necessary for the performance of the contract as stipulated

932 C-524/06 *Huber*, para 52.

933 See, e.g., C-13/16 *Rīgas satiksme*, para 30 and C-252/21 *Meta Platforms and Others*, para 93.

934 See, e.g., CJEU cases C-73/07 *Satakunnan Markkinapörssi Oy and Satamedia Oy*, para 56, C-92/09 and 93/09 *Volker und Markus Schecke and Eifert*, paras 77 and 86, C-473/12 *IPI*, para 39, C-293/12 *Digital Rights Ireland*, para 52, and C-212/13 *Ryneš,* para 28.

935 See, e.g., C-252/21 *Meta Platforms and Others*, para 108 and the case-law cited. See also (EDPB 2024a, 12). In its opinion on certain data protection aspects related to AI models, the EDPB has divided the necessity analysis into two points, as follows: '(i) whether the processing activity will allow the pursuit of the purpose; and (ii) whether there is no less intrusive way of pursuing this purpose', see (EDPB 2024b, 22–23).

936 See, e.g., (WP29 2018a, 13; EDPB 2019a, 8–10; 2024a, 12).

937 GDPR Recital 39. See, e.g., C-394/23 *Mousse*, paras 27-28, C-92/09 *Volker und Markus Schecke*, para 86 and C-439/19 *Latvijas Republikas Saeima*, para 113. See also (Kelly-Lyth 2021, 910–11).

938 For instance, *Kelly-Lyth* has considered it difficult for employers to show that automation of recruitment is necessary if the same recruitment activities have been previously conducted without using an automated system (Kelly-Lyth 2021, 910).

939 For national examples of such requirements, see (Publication I / Viljanen and Parviainen 2022, 3).

in GDPR Article 6(1)(b).[940] However, some circumstances might necessitate ARS use. First, if human recruiters cannot reasonably process a particularly high volume of applications, the ARS could be the least rights-intrusive option and necessary to enter into an employment contract.[941] Second, if ARSs are proven to be less biased than human recruiters, the necessity could be more readily established also from the perspective of GDPR Article 6.[942]

Applying the necessity requirement to ARSs requires, in practice, that employers assess the effects of the ARS on job applicants' fundamental rights. Further, employers must consider other available recruitment methods, including human-conducted recruitment, and their fundamental rights implications, to determine which is the least rights-restrictive option.[943]

In addition to the necessity requirement, the lawful basis of legitimate interests imposes two further cumulative conditions established in CJEU case law: the employer must be pursuing a legitimate interest, and it must conduct a proportionality assessment to ensure that its interests are not overridden by the job applicants' interests or fundamental rights and freedoms.[944] Together, these form the three cumulative conditions for utilising the lawful basis of legitimate interest under GDPR Article 6(1)(f): (i) pursuit of legitimate interests; (ii) necessity; and (iii) proportionality. The GDPR does not specify which interests qualify as legitimate.[945] The EDPB has considered that legitimate interests could cover a broad range of situations where the interests are lawful, clearly and precisely articulated, and real and present.[946] In prior research, *Kelly-Lyth* has suggested that the legitimate interests in the algorithmic hiring context could include, for example, removing strict gatekeeping measures and reviewing more applications, freeing human recruiters' time for personal encounters with the applicants, increasing the performance of new hires, and adding diversity to the workforce.[947] The proportionality condition further requires that the job applicants' interests or fundamental rights and freedoms do not take precedence over the employer's legitimate interests for that basis to be sufficient

940 (WP29 2018a, 13).
941 Similarly also in (Kelly-Lyth 2021, 911).
942 Of the necessity requirement and the less biased algorithmic systems in the context of indirect discrimination, see (Kelly-Lyth 2023, 157–59).
943 Hence, while GDPR Art. 6 concretises the fundamental right enshrined in CFREU Art. 8, it also has effects akin to the horizontal meta-effect approach, requiring employers in practice to consider job applicants' fundamental rights prior to adopting ARSs.
944 See, e.g., C-252/21 *Meta Platforms and Others*, para 106 and the case-law cited. See also (EDPB 2024a; Warter 2025, 181–83; Kelly-Lyth 2021, 910).
945 See also (EDPB 2024a, 7).
946 (EDPB 2024a, 7–8; 2024b, 21–22).
947 (Kelly-Lyth 2021, 906–7).

to legitimate the use of ARS under GDPR Article 6(1)(f).[948] The fulfilment of the proportionality requirement is assessed via a balancing test.[949]

The EDPB guidelines on legitimate interests provide a methodology for the balancing test.[950] Numerous case-specific factors must be considered, including the employers' legitimate interests, job applicants' interests, fundamental rights and freedoms concerned,[951] the impact of the processing on job applicants, their reasonable expectations regarding the processing,[952] and any additional safeguards adopted to prevent ARSs' impacts on applicants.[953] After weighing these factors, the employer must objectively balance all the identified interests, rights, and freedoms, which is not a straightforward task in any context.[954]

ARSs present a particularly demanding case for the balancing test, given their capability to process vast amounts of personal data and infer sensitive characteristics, and the resulting significant consequences for various fundamental rights.[955] They can also substantially affect the social and financial interests of vulnerable job applicants, even if applicants were informed of the ARS's use.[956] These considerations mean that

948 (EDPB 2024a, 5).

949 (EDPB 2024a, 13–19; WP29 2014, 33–42).

950 (EDPB 2024a, 13–19).

951 The EDPB has highlighted that data subjects' interests should be interpreted broadly to include any interest affected by the processing (e.g. financial, social or personal interests) and the fundamental rights to be considered extend beyond data protection and privacy to encompass other fundamental rights and freedoms (EDPB 2024a, 13). This broad interpretation is reflected in the EDPB's opinion on AI models, which identifies as potentially affected interests and fundamental rights in the deployment phase: data subject interests in retaining control of their personal data, financial interests, personal benefits and socioeconomic interests, and as regards fundamental rights, the opinion mentions among others, the rights to privacy, to the protection of personal data, to engage in work and to non-discrimination (EDPB 2024b, 24).

952 GDPR Recital 47 emphasises the importance of considering data subjects' reasonable expectations in the balancing test. The EDPB states in its opinion 28/2024 that the complexity of technologies used in AI models makes it more difficult for data subjects to understand the use cases and data processing involved. Accordingly, this highlights the role of reasonable expectations in the balancing test (EDPB 2024b, 26–27).

953 See, e.g., (EDPB 2024a, 13–19). As regards additional safeguards, the EDPB has repeatedly emphasised that they should go beyond what is legally required to comply with the GDPR (EDPB 2024a, 19; 2024b, 28). EDPB suggests that publishing the balancing test could be one mitigating measure (EDPB 2024b, 30).

954 See also (EDPB 2024a, 18–19).

955 As discussed above in sections 1.1.1, 1.3.2 and 3.1, ARSs may affect not only the rights to data protection and privacy, but also equality and access to employment among others.

956 Of the effects of ARSs, see, e.g., (Rigotti and Fosch-Villaronga 2024, 3; Sánchez-Monedero et al. 2020, 2–3; Parodi 2024, 122; Hunkenschroer and Luetge 2022, 993–98; Hunkenschroer and Kriebitz 2023, 204; Giermindl et al. 2022, 414, 418, 423–24; Kelly-Lyth 2021, 903–4). See also (EDPB 2024b, 24).

the employers' legitimate interests must carry considerable weight, not to be overridden by the job applicant's rights and interests, and thus to qualify as a lawful basis for processing personal data in an ARS. Two factors could support employers' claims that their interests are sufficiently weighty. First, the more beneficial the ARS is for job applicants, such as through less biased hiring outcomes and faster processes, the more readily the processing could be based on legitimate interests.[957] Second, the more limited the scope of the processing by ARS, such as conducting only basic eligibility checks, the more easily it could be justified. By contrast, more expansive processing, such as AI-based video interviewing that generates vast and varied personal data, including potentially sensitive data, faces a considerably higher threshold.

In sum, employers should carefully consider whether they have a lawful basis for all the processing of personal data within the ARS.[958] The most likely lawful bases are the necessity for entering into an employment contract and the necessity for the employer's legitimate interests.[959] Nevertheless, the ARSs could involve certain processing activities, such as in-depth analysis of job applicants' social media profiles and online behaviour, for which a lawful basis might not exist. Consequently, the obligation to demonstrate lawful grounds for processing personal data could limit the feasibility of some technologically possible features of the ARSs.

Further constraints are imposed by the GDPR Article 5 principles relating to processing of personal data. Compliance with GDPR Article 5 is likely to be harder to assess and demonstrate in ARSs than in traditional recruitment, not least because of ARSs' complexity, opacity and employers' limited knowledge of how they operate.[960]

Especially, the principle of lawfulness, fairness and transparency in GDPR Article 5(1)(a) could set high standards. It requires not only that the processing complies with the GDPR overall, but also that it complies, for instance, with non-discrimination legislation and the requirements of the AIA, where applicable to the

957 See also (EDPB 2024b, 25; Kelly-Lyth 2021, 910).

958 See also (ICO 2024, 44–45).

959 Of the centrality of the legitimate interests in the context of algorithmic management in general, see, e.g., (Warter 2025, 181). However, even if the employer initially concludes that it has legitimate interests to process job applicants' personal data within the ARS, the applicants may object to the processing under GDPR Art. 21(1). After an objection, the processing may continue only if the employer demonstrates compelling legitimate grounds for continuing that override the interests, rights and freedoms of the data subject. Of the right to object, see also (EDPB 2024a, 21–22) and section 5.2.4 below.

960 Of the problems, especially as regards profiling and ADM, see (WP29 2018a, 9–12) and regarding AI systems in general, see, e.g., (Drouard et al. 2024b).

ARS.[961] As was briefly mentioned in section 5.2.1.2 above, the EDPB has suggested that compliance with the principle of lawfulness would extend to ascertaining the lawfulness of the processing of personal data in the development phase, if personal data is retained in the AI model.[962] According to the EDPB, to verify the lawfulness of processing, the controller should consider the sources of personal data used in the development phase and whether any infringements have been found in prior proceedings.[963] Since ensuring the lawfulness of processing personal data in the development phase can be particularly difficult for employers, where possible, they should adopt AI systems that rely on anonymous AI models.[964]

The GDPR does not explicitly state what the fairness principle comprises.[965] It is often mentioned in relation to both lawful[966] and transparent[967] processing.[968] The EDPB has stated that the principle of fairness requires that personal data is not processed by 'unfair methods, [...] deception, or in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data subject'.[969] Hence, the fairness principle demands, among others, recognising the data subjects' reasonable expectations, considering possible adverse effects on data subjects and noting the nature of the relationship between the controller and the data subject.[970] In the context of ARSs, the fairness principle could encompass even broader requirements than lawfulness, for instance, as regards the correlations used. Certain data points may not be considered discriminatory under non-discrimination legislation,

961 The principle of lawfulness brings some of the AIA's requirements set on the providers also to the sphere of deployer's responsibility, such as the below-discussed transparency requirements, CE-marking and registration requirements. On the extent of GDPR Art. 5(1)(a) in the context of AI systems, see (EDPB 2024b).

962 (EDPB 2024b, 4 and 34). The EDPB appears to suggest that this could also be required for complying with GDPR Art. 6 in the use phase.

963 (EDPB 2024b, 4 and 34).

964 The EDPB has considered that for an AI model to be anonymous, 'both (1) the likelihood of direct (including probabilistic) extraction of personal data regarding individuals whose personal data were used to develop the model and (2) the likelihood of obtaining, intentionally or not, such personal data from queries, should be insignificant, taking into account 'all the means reasonably likely to be used' by the controller or another person.' (EDPB 2024b, 2, 14–19). Cf. (Hamburg Commissioner for Data protection and freedom of information 2024).

965 CFREU Art. 8(2) also notes that personal data must be processed fairly. Of the vagueness, unclarity and history of fairness, see also (Malgieri 2020, 155; Clifford and Ausloos 2018).

966 See, e.g., GDPR Art. 6(1)(c) and (e) and Recitals 39 and 45.

967 See, e.g., GDPR Arts. 13(2) and 14(2), and Recitals 39, 60 and 71.

968 Yet, for instance, *Alessandro Malgieri* has stated that the principle of fairness also has an independent meaning (Malgieri 2020, 156).

969 (EDPB 2024b, 19–20). See also (EDPB 2024c, 5 and 15; 2020a, 17–18).

970 (EDPB 2019a, 6). See also (Rigotti and Fosch-Villaronga 2024, 5–6).

but their use could still be deemed unfair from the perspective of job applicants. *Lilian Edwards and Michael Veale* have questioned arbitrary correlations (e.g. web browser preferences as a predictively useful variable) based on this principle.[971] Yet, ensuring that such miscellaneous unfair variables are not used could be even more difficult than preventing discrimination based on the listed protected grounds.

Moreover, the principle of transparency is a core obligation in the GDPR.[972] According to the WP29, the transparency principle aims to ensure that data subjects know in advance the scope and consequences of processing, so that they are not later surprised by the use of their personal data.[973] In the algorithmic recruitment context, this principle operates on several levels. It requires that job applicants are informed of the extent to which their personal data is or will be processed,[974] that this information is easily accessible, easy to understand, and provided using clear and plain language,[975] and that employers facilitate the exercise of data subject rights.[976] The detailed information obligations discussed below give concrete expression to this principle,[977] and should be read in light of it.[978] Transparency is also crucially linked to accountability and fairness,[979] enabling job applicants to understand and, where necessary, challenge the processes that affect them.[980]

Achieving transparency is, however, particularly challenging where an intractable ARS is used, as its complexity and opacity may make it difficult to ensure transparency in practice and demonstrate compliance with GDPR's requirements. It remains to be seen how strictly the CJEU will interpret the transparency principle in the context of AI and algorithmic decision-making, and consequently how constraining an obligation it will ultimately impose on employers using ARSs.

The principle of purpose limitation under GDPR Article 5(1)(b)[981] requires that personal data is 'collected for specified, explicit and legitimate purposes and not

971 See (Edwards and Veale 2017, 30; The Economist (Online) 2013). See also (EDPB 2024b, 19–20).
972 (WP29 2018c, 4).
973 (WP29 2018c, 7).
974 GDPR Recital 39. See also (WP29 2018c, 4).
975 GDPR Recital 39. GDPR Art. 12(1) specifies that the information and communication provided to the data subject must be 'in a concise, transparent, intelligible and easily accessible form, using clear and plain language'. See also (WP29 2018c, 4; 6–10; EDPB 2024b, 20).
976 (WP29 2018c, 4).
977 (WP29 2018c, 5).
978 See GDPR Arts. 12–22 and 34, as well as CJEU case law regarding those below in section 5.2 and section 6.1.2.
979 (WP29 2018c, 5).
980 (WP29 2018c, 4). Similarly, also in (EDPB 2020a, 15).
981 CFREU Art. 8(2) also notes that personal data must be processed for specified purposes.

further processed in a manner that is incompatible with those purposes'.[982] Despite the wide processing possibilities ARSs may allow, employers must therefore define a specific and explicit purpose for the processing of job applicants' personal data.[983] Employers must ensure, on the one hand, that job applicants' personal data collected and processed by the ARS is used only for the specified recruitment purposes and not in an incompatible manner, for instance, for developing internal AI systems.[984] On the other hand, employers must verify that the personal data processed by the ARS does not originate from sources where the data has been collected for incompatible purposes.[985] For example, the employer may wish to utilise performance evaluations of current employees seeking other positions within the company. Such further processing must be assessed on a case-by-case basis, taking into account the criteria listed in GDPR Article 6(4), including the information initially provided to job applicants, the relationship between the purposes, job applicants' reasonable expectations, the type of personal data, the impact of further processing, and the safeguards adopted.[986] In line with the transparency principle, if the employer intends to process personal data for another purpose, it must inform the job applicant in advance[987] and explain how the further processing is compatible with the original purposes, as guided by the WP29.[988]

982 The GDPR does not elaborate on what the specified, explicit and legitimate mean in this context. The WP29 has stated in its Opinion 03/2013 on purpose limitation that being specified means that the purpose must be sufficiently defined to allow implementation of data protection safeguards and limit the scope of the processing. According to WP29, explicit means that the purpose must be 'sufficiently unambiguous and clearly expressed', while legitimacy goes further than having a lawful basis under GDPR Art. 6, extending also to other applicable law, including non-discrimination. See (WP29 2013, 12). Although the EDPB has not endorsed the WP29 Opinion on purpose limitation, EDPB has deemed it still possibly relevant as the wording of the principle under the former Data Protection Directive (95/46/EC) was the same as under the GDPR, see (EDPB 2020a, 19).

983 See also (EDPS 2025, 22–23), where this question is discussed from the perspective of EU institutions and generative AI-supported recruitment.

984 See also (ICO 2024, 7–8).

985 There might also be more specific requirements on this in MS legislation, such as the Finnish Act on Protection of Privacy in Working Life (759/2004), Section 4, which requires that, as a rule, personal data should be collected from the employee or job applicant themselves, and only with their consent from other sources. However, Section 4 specifies some exceptions, including authorities' information disclosures for fulfilling statutory duties and separate express provisions in other legislation.

986 See GDPR Art. 6(4) and (WP29 2018a, 11; 2013, 21–23; Drouard et al. 2024b, 305–7).

987 GDPR Arts. 13(3) and 14(4). See also (WP29 2018c, 23–24).

988 (WP29 2018c, 24).

Overall, ARSs may increase the temptation to maintain extensive databases of employee and applicant information, to further develop the ARSs, and to make more informed employment decisions.[989] In addition to the purpose limitation, the principles of data minimisation and storage limitation also considerably limit such aspirations. The principle of storage limitation requires that when the personal data is no longer necessary for the purposes of its processing, it should be removed or anonymised.[990] In the recruitment context, it might be argued, especially if the job applicant has shown their eagerness to be employed in other positions within the organisation, that the application and CV may be needed to fill further job openings.[991] However, this period may not be very long, as the information in those documents could change once the applicant obtains additional qualifications and experience.[992]

The data minimisation principle limits the use of ARSs to only such personal data that is adequate, relevant and necessary for making the recruitment decisions.[993] To be considered necessary, the purposes of processing should not be reasonably fulfilled without processing that particular personal data.[994] The EDPB has stated that the controller must verify whether the purposes can be reached by processing less personal data, less detailed or aggregated personal data, or with no personal data at all.[995] Hence, the employers should be able to justify why the use of certain personal data is necessary for the recruitment decision-making. For instance, relevant and necessary personal data is that which is required to assess job applicants' competence and suitability for the position. Since the required data may vary by position, it cannot be exhaustively defined at the system level.

Implementing the data minimisation principle could, for instance, require guidance or warnings for recruiters and job applicants entering their information into the system, to avoid inputting unnecessary personal data.[996] Further, it could limit the usability of certain ARS features, such as extensive scraping of publicly available data on social media profiles.[997] Ensuring full compliance is, however, more difficult

989 (WP29 2018a, 11). Of this risk, see also (Barberá 2025, 55; ICO 2024, 16).
990 GDPR Art. 5(1)(e), which contains exceptions for archiving purposes.
991 See also (EDPB 2026).
992 See also (ICO 2024, 15–16; WP29 2017b, 11).
993 GDPR Art. 5(1)(c). For example, in the above-discussed browser example, this principle links closely to the fairness principle.
994 See GDPR Recital 39 and (de Terwangne 2020, 317).
995 (EDPB 2020a, 21).
996 For a similar suggestion, see also (Barberá 2025, 29). There are various technical means to ensure data minimisation. For example, *Etienne Drouard et al.* have suggested continuous data assessments and dynamic data minimisation techniques to ensure data minimisation is at the required level (Drouard et al. 2024a, 176).
997 See also (WP29 2017b, 11).

where ARSs are complex and opaque. Such ARSs may based on input data draw unnecessary inferences that remain out of employers' sight, thereby limiting their ability to independently verify compliance. Nevertheless, at a minimum, employers should ensure that, based on the information available to them[998], no unnecessary personal data is processed and data minimisation is addressed in their contract with the ARS provider.[999]

Moreover, the personal data processed by the ARS should be accurate and kept up to date.[1000] The EDPB has pointed out that one element to be considered is the degree of accuracy, meaning that personal data should be 'as accurate as necessary for the specified purposes'.[1001] In the recruitment context, the stakes are high, as applicants' professional futures and incomes, among other factors, are on the line. This increases the importance of making decisions based on accurate data. For employers, this means confirming that the personal data the ARSs process is accurate at all stages of the recruitment process.[1002] Keeping the input data accurate and updating it when necessary could be the easiest part.[1003] However, even when provided with accurate input data, ARSs' deficiencies, such as confabulations inherent in LLM-based recruitment systems,[1004] might lead to the processing of inaccurate personal data.[1005]

Should any inaccuracies in the personal data processed be discovered, employers must take every reasonable step to promptly erase or rectify such inaccuracies.[1006] Rectification is crucial, as inaccurate or outdated personal data likely leads to flawed decisions or profiles, to the detriment of both employers and job applicants.[1007] In

998 Employers must primarily rely on the information the ARS providers provide them about the ARS, for instance, in their marketing materials, contract negotiations, and instructions for use. See, e.g., AIA Art. 13, which requires providers to accompany high-risk AI systems with instructions for use.

999 The ARS providers could often be better positioned to ensure that the ARS complies with the data minimisation principle. See also (ICO 2024, 16).

1000 GDPR Art. 5(1)(d).

1001 (EDPB 2020a, 23).

1002 (WP29 2018a, 12). However, analysing the accuracy of the ARS output appears to fall outside the scope of data protection law, see C-434/16 *Nowak*, para 57 and (Wachter and Mittelstadt 2019, 499–500).

1003 Ensuring that the inferences drawn by the system are accurate is much more complicated, especially when employers do not fully understand the logic according to which the ARS operates. Job applicants' possibilities to ensure the accuracy of the inferences could also be limited. See also (EDPB 2024c, 8).

1004 See also (Christakis 2024). Measures to challenge the LLMs' confabulations have been initiated, see, e.g., (noyb 2024). For more detailed discussion, see section 3.3.2 above and section 6.2 below.

1005 (WP29 2018a, 17).

1006 GDPR Art. 5(1)(d).

1007 (WP29 2018a, 12).

high-risk decision-making contexts[1008] such as recruitment, however, mere ex-post rectification may not be sufficient, as many decisions could proceed to execution before inaccuracies are noted, thereby risking job applicants' fundamental rights to data protection and non-discrimination. Instead, an interpretation that regards the principle of accuracy as prohibiting the high-risk use of systems known to be inaccurate, despite mitigation measures, would more effectively safeguard the high level of data protection that the GDPR seeks to guarantee.[1009] Accordingly, rather than demanding rectification in the few cases where the confabulations are detected, the principle of accuracy could be read to require that the inaccuracies be avoided in the first place.

This teleological interpretation would significantly constrain the use of LLM-based recruitment systems that are prone to confabulations.[1010] However, design solutions may allow their use, at least to some extent. For instance, LLM-based recruitment systems designed to create summaries of CVs and applications for human recruiters could present those summaries to applicants already at the point of submission. Applicants could then verify the accuracy of the summary and flag any discrepancies before the process continues. Such a procedure could ensure the accuracy of LLM-generated summaries, enabling their use in the recruitment process.

The last of GDPR Article 5(1) principles requires that personal data is processed in a way that ensures the appropriate security of the personal data. In practice, appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss, destruction or damage are required of the employer. There are regrettable examples of recruitment systems leaking millions of job applicants' personal data due to very basic security flaws.[1011] In recruitment processes, the volume of personal data processed can be considerable, increasing the risks associated with such breaches. In prior accounts, it has been suspected that LLM-based systems would further increase the risk of unauthorised disclosure of personal data, which emphasises the importance of taking this principle seriously.[1012] The measures employers should adopt could include, among others, proper risk

1008 Of the importance of the context in considering the accuracy requirements in relation to confabulations, see also (Christakis 2024, 2).

1009 GDPR Art. 1 and Recitals 1, 2 and 6. The EDPB's ChatGPT Taskforce emphasised that the principle of accuracy must be complied with also in the context of ChatGPT (EDPB 2024c, 8). Yet, what that requires in practices remains still to be seen.

1010 Measures to mitigate confabulations have been taken, see, e.g., (Christakis 2024, 7–10). Yet, it remains unclear whether confabulations will ever be completely preventable in LLMs, see, e.g., (Huang et al. 2024, 2–4; Banerjee et al. 2024, 1).

1011 For instance, tens of millions of McDonald's job applicants' personal data was reported to be leaked due to the use of the password '123456', (Greenberg 2025).

1012 Of attacks with prompts to obtain personal data, see, e.g., (Engel et al. 2023, 2; Carlini et al. 2023; EDPB 2024b, 18).

analysis, regular reviews and tests of the system, access control management and backups.[1013]

The employer is responsible for and must demonstrate compliance with the principles of data processing as required by GDPR Article 5(2). In practice, this requires the adoption of appropriate technical and organisational measures, including due diligence processes and contractual arrangements with relevant actors in the ARS's lifecycle, as well as the integration of necessary safeguards to protect job applicants' rights and freedoms.[1014] The EDPB guidelines on data protection by design and by default list several technical and organisational measures that employers could consider establishing to effectively implement the data protection principles.[1015] In line with GDPR Article 25, data protection requirements should be noted already at the planning stage and continually throughout the processing.[1016]

When the ARS is not developed in-house, compliance begins with a thorough pre-adoption due diligence.[1017] This process should encompass several elements. The provider should be able to show how it has acknowledged and ensured the fulfilment of the data protection principles when developing the ARS. Further, the WP29 has recommended obtaining contractual assurances which confirm that auditing and testing have been carried out and that the system complies with agreed standards.[1018] The employer should also require the ARS provider to act transparently and cooperate with the employer, thereby enabling compliance with the employer's obligations under the GDPR and the AIA. The due diligence conducted at the acquisition stage could also assist the employer in fulfilling other duties, such as conducting a DPIA.[1019] However, pre-adoption verification alone is insufficient, and regular compliance checks should subsequently be conducted to ensure that the provider has implemented the necessary measures to maintain compliance.[1020]

In addition to adhering to the principles governing the processing of personal data, the employer must ensure that the use of an ARS allows the fulfilment of job applicants' rights under the GDPR.[1021] Equally, fulfilling job applicants' rights can

1013 For a more detailed list of elements to potentially include in implementing the integrity and confidentiality principle, see, e.g., (EDPB 2020a, 26–27).
1014 GDPR Arts. 24 and 25. In addition to the contracts with the providers, also the contracts with possible processors of personal data should note these requirements (GDPR Art. 28).
1015 (EDPB 2020a).
1016 See also (EDPB 2020a, 4).
1017 (ICO 2024, 40).
1018 (WP29 2018a, 32).
1019 Of this duty see GDPR Arts. 35 and 36 and section 5.2.3 below.
1020 (ICO 2024, 40).
1021 See GDPR Art. 12.

serve as a means of enhancing compliance with the general principles of processing.[1022] Within the framework of key legal parameters, the general rights established in GDPR Chapter 3 have been categorised into two distinct categories. Rights which do not require job applicants' active measures are deemed as obligations. In contrast, rights that require invocation by job applicants comprise a distinct category of actionable rights, which will be discussed in more detail in section 5.2.4 below.[1023]

Job applicants' rights to information about the processing of their personal data are crucial for ensuring transparency.[1024] Employers must actively provide this information to the job applicant. The WP29 has instructed that it could be done either by furnishing them with the information or actively directing them to its location, for instance, through a direct link.[1025] The information to be provided differs depending on the type of ARS, as specific information about the system is required under the GDPR only in case the system conducts ADM.[1026] In other ARSs, only more general information about the processing of job applicants' personal data, such as the purposes of the processing, its legal basis, and job applicants' rights under the GDPR, must be provided.[1027] Although the GDPR does not explicitly require that job applicants be informed of ARS use where it does not involve ADM, the WP29 has deemed it would be a good practice.[1028] A stronger case could be made on the basis of the principles of fairness and transparency. The Information Commissioner's Office (ICO) has considered that processing would be effectively invisible if people are not informed how their personal data is processed within AI tools,[1029] suggesting that disclosure of ARS use may in fact be required as a matter

1022 For instance, the right of access (GDPR Art. 15) and the right to rectification (GDPR Art. 16) could assist in securing the accuracy of the personal data processed. See also (WP29 2018a, 17).

1023 Similarly, in its guidelines on automated decision-making and profiling, the WP29 has noted that some data subject rights require active exercise, whereas others are passive and do not require data subjects to take action. See (WP29 2018a, 34).

1024 GDPR Arts. 13 and 14 and Recital 63. The WP29 has also emphasised the importance of transparency in the context of profiling and automated decision-making (WP29 2018a, 24–25).

1025 (WP29 2018c, 18).

1026 GDPR Art. 13(2)(f) and 14(2)(g). This obligation will be discussed in more detail below in section 5.2.3. The specific duties stemming from the AIA in the case of using high-risk AI systems complement this information.

1027 GDPR Arts. 13 and 14. For detailed guidance on what information to provide, see (WP29 2018c, 35–40). As regards informing about the particular legitimate interests relied upon and of informing about the balancing tests upon request, see also (EDPB 2024a, 20–21).

1028 (WP29 2018a, 25).

1029 (ICO 2024, 27).

of principle rather than merely recommended. Nevertheless, the principle of transparency and the information obligations outlined in GDPR Articles 12–14 are unlikely to impose overly detailed ex-ante information obligations that would directly constrain the use of intractable ARSs.

Similarly to the GDPR-based qualified bans, breaches of the GDPR's obligations could result in an administrative fine of 20 million euros or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[1030] and the data protection authorities may use their powers to prevent the breaches from continuing.[1031]

However, the GDPR is not the only EU legal instrument that imposes obligations for all ARSs. The reasonable accommodation obligation in Article 5 of the EED must also be observed. It requires that, when necessary in a particular case, employers take appropriate measures to enable a person with a disability[1032] to have access to employment, unless such measures would impose a disproportionate burden on the employer.[1033] Although under EU law, the duty of reasonable accommodation is triggered only when the employer becomes aware of a person's disability, in practice, it should be considered from the outset when developing or procuring ARSs.[1034] In the algorithmic recruitment context, the duty to provide reasonable accommodations could require both system-level design considerations[1035] and individual adjustments in particular cases.[1036] Hence, this duty shapes ARSs by effectively requiring them to include accessibility features, such as compatibility with assistive technologies (e.g., screen readers or speech recognition) or time

1030 GDPR Art. 83(5).

1031 See section 5.2.1.2 above for a discussion on the authorities' enforcement possibilities.

1032 The EED lacks a definition of disability, but it has been conceptualised by the CJEU. The first conceptualisations relied on a medical model of disability independent of external or environmental factors, see case C-13/05 *Chacon Navas*, para 43. See also (Kelly-Lyth 2023, 164; Tilmes 2022, 2). However, in later cases, the CJEU has adapted its conceptualisation to be more contextual, noting also other barriers that may hinder full and effective participation in professional life, see C-335/11 and C-337/11 *HK Danmark*, para 38. In recruitment, the use of an ARS could be a conceptual factor, affecting the analysis of disability.

1033 According to EED Recital 21, when considering whether there is a disproportionate burden, for instance, financial and other costs entailed, scale and financial resources of the organisation should be noted.

1034 (Kelly-Lyth 2023, 166; Daly and Whelan 2021, 750; Buyl et al. 2022, 1074–75). Referring to *Daly and Whelan*, *Kelly-Lyth* has argued that using a tool that lacks accessibility functions could constitute indirect discrimination if its use 'unjustifiably disadvantages persons with disabilities and there are equally effective alternatives reasonably available' (Kelly-Lyth 2023, 166; Daly and Whelan 2021, 750).

1035 See, e.g., (Tilmes 2022, 21–23).

1036 (Kelly-Lyth 2023, 164).

extensions.[1037] Ensuring that such functions exist in the ARSs should not be disproportionate for employers that have the resources to utilise ARSs in the first place.[1038] However, regardless of the existence of such basic accessibility functions, the employer must, in individual cases where it becomes aware of a job applicant's disability, evaluate whether those measures are sufficient and what additional measures might be needed.[1039] The sanctions for breaching the duty of reasonable accommodation are left to the discretion of the Member States.[1040]

Obligations regarding AI systems

When the ARS is considered an AI system, there are three general obligations that employers should note as of 2nd August 2026.[1041] First, if the ARS generates deepfakes,[1042] AIA Article 50(4) requires that employers disclose that the content has been artificially generated or manipulated.[1043] Recital 134 further clarifies that the disclosure should be done clearly and distinguishably by labelling the AI output accordingly and disclosing its artificial origin. While it is possible that the ARSs could create deepfakes, those are typically not the primary functions of the systems.[1044] Thus, instead of constraining the use of ARSs, this obligation appears to impose just another transparency requirement for employers to comply with. AIA Article 50(4) also requires disclosure of AI-generated or manipulated text which is published with the purpose of informing the public on matters of public interest. When the ARS generates text for the purposes of informing, the text is typically for

1037 See EED Recital 20 and (Kelly-Lyth 2023, 165; U.S. Equal Employment Opportunity Commission 2022).

1038 For instance, *Patrick Daly and Darius Whelan* have pointed out that the disproportionate burden defence could lead to lesser protection where employers have minimal financial resources (Daly and Whelan 2021, 746–47).

1039 *Maarten Buyl et al.* have, for instance, suggested the possibility of opting out of the ARSs (Buyl et al. 2022, 1075).

1040 EED Art. 17.

1041 AIA Art. 113.

1042 According to AIA Art. 3, point 60, deepfakes are 'AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful'. See also Recital 134. For a more detailed analysis of the criteria set for deep fakes, see, e.g., (Gils 2024, 803–4).

1043 There is one exception to this disclosure obligation relating to law enforcement purposes and one alleviation regarding evidently creative or satirical works, where the disclosure of the artificial origin can be done in an appropriate manner which does not impede the display or enjoyment of the work (AIA Art. 50(4)).

1044 Deepfakes could be problematic also when used by the job applicants to deceive in the hiring decision-making or if malicious actors use deepfakes to tarnish the hiring company's reputation, see (Sharma 2024).

commercial purposes and not relating to a matter of public interest. Thus, this latter obligation is not likely to be triggered in ARSs.

Moreover, most of the AIA's obligations are not explicitly directed at AI system deployers, but employers may have the obligation to ensure that those are complied with to ensure general lawfulness as required by GDPR Article 5(1)(a). If personal data is processed by an AI system that clearly does not comply with the AIA, its lawfulness could be questioned. Hence, when acquiring ARSs employers should, as part of their due diligence processes,[1045] verify that a high-risk AI system they deploy is CE-marked[1046] and registered in the EU database for high-risk AI systems,[1047] which is an important additional avenue of information for job applicants.[1048] Furthermore, if the ARS interacts directly with job applicants, the employer must ensure that the system they use complies with the transparency obligations set out in AIA Article 50(1).[1049] The information needed to verify these points is readily available to the employer, making verification feasible despite employers' limited access to system documentation and their limited understanding of the underlying mechanisms.[1050]

The sanctions for breaching the explicit deployer's duties under AIA Article 50(4) could result in similar administrative measures, as discussed above in relation to the AIA's bans on specific practices. The administrative fines in these cases could be up to 15 million euros or 3 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (or lower for SMEs).[1051] As regards the other AIA-related obligations discussed in this part, a potential breach could concern GDPR Article 5(1)(a) and mirror the sanctions discussed above in relation to the GDPR's obligations.

Obligations regarding ADM

GDPR Article 22(3) requires that where an ARS makes automated decisions, employers must ensure that suitable safeguards are in place to protect job applicants' rights, freedoms and legitimate interests.[1052] At a minimum, these safeguards must

[1045] The EDPB opinion suggests that even more far-reaching due diligence could be required of deployers when they are taking AI systems into use (EDPB 2024b, 33–34).
[1046] AIA Art. 48.
[1047] AIA Arts. 49 and 71.
[1048] (Publication IV / Parviainen 2026). See also section 6.1.2.2 below.
[1049] AIA Art. 50. See also (Veale and Zuiderveen Borgesius 2021, 107).
[1050] Apart from marketing materials and other publicly available information, deployers are not necessarily offered access to anything other than instructions for use (AIA Art. 13) and logs (AIA Art. 12).
[1051] AIA Art. 99(4).
[1052] GDPR Art. 22(3) requires that 'data controller shall implement suitable measures'.

include the right to obtain human intervention,[1053] express their point of view and contest the automated decision.[1054] The list is not exhaustive, however, and the GDPR anticipates a broader range of protective measures. GDPR Recital 71 elaborates on this, mentioning among other safeguards the provision of specific information to the data subject, the right to obtain an explanation of the decision reached, appropriate mathematical and statistical procedures for profiling, technical and organisational measures to ensure correction of inaccuracies and minimise error risks, security measures and the prevention of discrimination.[1055] Beyond the GDPR's own enumeration, the WP29 has suggested further good safeguard practices for controllers, including regular quality assurance checks to ensure fairness and non-discrimination, algorithmic auditing and testing, independent 'third party' auditing, and anonymisation and pesudonymisation techniques.[1056]

The safeguards serve a dual role: preventing unlawful decisions *ex ante*[1057] and enabling the verification, overruling, and challenging of automated decisions *ex post*.[1058] Accordingly, the safeguards are noted in the framework of key legal parameters as both obligations and actionable rights.[1059] All the safeguards, but especially the additional ones mentioned in Recital 71, could be viewed as procedural measures that employers must ensure are built into their recruitment processes and enabled through sufficient transparency.[1060] The human intervention obligation illustrates this concretely: when adopting ARSs with ADM capabilities, employers should assign a competent and authoritative person to handle job applicants' cases[1061] and ensure that the ARSs used are sufficiently understandable to allow those persons to exercise meaningful oversight.[1062] Hence, the suitable safeguards could shape both the recruitment processes conducted utilising ARSs and

1053 When the ARS is a high-risk AI system, this requirement should be read together with AIA Art. 14, which will be discussed in some more detail in subsection 5.3.3. See also (Lazcoz and de Hert 2022).

1054 GDPR Art. 22(3).

1055 This Recital's role has been debated in scholarship, see e.g. (Wachter et al. 2017, 80; Malgieri and Comandé 2017, 255; Kaminski 2019, 195; Wachter and Mittelstadt 2019, 569).

1056 (WP29 2018a, 32).

1057 See (Brkan 2019a, 107).

1058 See (Dreyer and Schulz 2019, 9–10; Wachter and Mittelstadt 2019, 569).

1059 In particular, the minimum safeguards listed in GDPR Art. 22(3) resemble actionable rights in their wording and are thus discussed in section 5.2.4 below.

1060 Of the importance of transparency in securing the safeguards of GDPR Art. 22(3), see case C-230/22 *Dun & Bradstreet Austria,* para 58.

1061 (WP29 2018a, 27). Similarly, also under AIA Art. 14.

1062 This interpretation stems from a combined reading with the AIA Art. 14, which will be discussed in some more detail in subsection 5.3.3. See also (Lazcoz and de Hert 2022).

the ARSs themselves. Failure to implement the required safeguards attracts the same sanctions as breach of the ban on ADM.[1063]

The minimum safeguard measures will be discussed in more detail in section 5.2.4, in connection with job applicants' actionable rights. Next, the focus shifts to the employers' specific duties.

5.2.3 Specific duties

The category of specific duties encompasses requirements imposed on employers that demand their proactive measures and do not arise in traditional, fully human-conducted recruitment processes. This distinguishes the specific duties from the obligations category, which includes, among other provisions, several overarching data protection obligations and the responsibility to provide reasonable accommodations, both of which apply regardless of how the recruitment process is conducted. However, the scope of the specific duties category is more limited, as many of its duties are based on the AIA and apply only to high-risk AI systems.

While allowing some flexibility in implementation, the specific duties impose more direct, concrete operational requirements on employers. Owing to their greater degree of concreteness, these duties may appear easier for the employers to comply with than the more general obligations. Whereas most of the general obligations are already in force, the majority of the specific duties will apply only to employers using such high-risk AI systems that are placed on the market or put into service as of 2nd August 2026.[1064] Systems made available before that date will fall under the AIA's high-risk provisions only if significant changes in their designs are made.[1065]

In any case, specific duties require active measures from employers using ARSs and are likely to shape both ARS adoption and operation processes. Compared with

1063 See section 5.2.1.2 above.

1064 However, AIA Art. 4 on AI literacy applies to deployers of all types of AI systems, and it has been applicable as of 2nd February 2025. The Commission's Proposal on Digital Omnibus on AI would extend this time limit further, so that the duties would be applicable 6 months after the adoption of the Commission's decision which confirms that adequate measures in support of compliance with AIA Chapter III are available, or on 2 Decmber 2027 at the latest.

1065 See AIA Art. 111(2) and (Publication IV / Parviainen 2026). See also AIA Recital 177, which clarifies that the significant change should be understood similarly as substantial modifications, which are defined in AIA Art. 3, point 23 as unforeseen or unplanned changes, not noted in the original conformity assessment, and as a result of which it affects the compliance of the AI system with the high-risk AI system requirements or modifies its intended purpose. Notably, if the deployer makes such substantial modifications to the ARS and it remains a high-risk system, the deployer will become the system's provider under AIA Art. 25(1).

the broader obligations, the constraining effects of the specific duties could be somewhat more limited. Nevertheless, the duty to conduct a data protection impact assessment could also amplify the effect of the other categories of legal parameters, as it establishes the currently only ex-ante external oversight mechanism for ARSs.

Specific duties for employers using any kind of ARS

Regardless of the ARS type, employers must determine whether a data protection impact assessment (DPIA) is required under GDPR Article 35(1). A DPIA must be completed before using the ARS if the processing is likely to result in a high risk to data subjects' rights and freedoms. When evaluating such risks, employers must consider the nature, scope, context, and purposes of the processing.[1066]

GDPR Article 35(3) explicitly identifies three situations in which a DPIA is required, but the list is not exhaustive.[1067] For instance, GDPR Article 35(3)(a) requires a DPIA in case of 'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'.[1068] The WP29 has interpreted this to apply also to decision-making that is not solely automated.[1069] Hence, for example, the use of ARS to automatically screen job applications could trigger the requirement to conduct a DPIA under GDPR Article 35(3)(a) even if humans are meaningfully involved in the process. Moreover, under GDPR Article 35(4), the national supervisory authorities must publicise lists of processing operations requiring a DPIA.[1070]

Where it is unclear whether a DPIA is required, the WP29 guidelines can provide assistance: it has identified nine criteria for evaluating processing risk, and the DPIA duty is generally triggered when at least two of those are met.[1071] The criteria most relevant to ARSs include evaluation and scoring, ADM with a legal or similarly significant effect, processing data concerning vulnerable data subjects,

1066 GDPR Recital 90 and (WP29 2017a, 14). For instance, *Kelly-Lyth* has considered the systems' possibility of being biased as giving rise to a high risk that triggers the DPIA requirement (Kelly-Lyth 2021, 915).

1067 See (WP29 2017a, 9).

1068 See also GDPR Recital 91. This formulation resembles AIA Art. 86.

1069 (WP29 2018a, 29).

1070 Based on GDPR Article 64(1)(a), the EDPB must issue an opinion on the national DPA's draft lists in order to harmonise the approach in cross-border matters and matters that can affect the free flow of personal data. See, e.g., (EDPB 2018b, 3).

1071 (WP29 2017a, 9–11). In its opinions issued on the national DPA's draft lists under GDPR Article 35(4), the EDPB appears to have also required two criteria in order to trigger the DPIA requirement, see, e.g., (EDPB 2018c, 7–8; 2018d, 8; 2019c, 6).

innovative use or application of new technological or organisational solutions, and processing that prevents data subjects from exercising their rights or using a service or contract.[1072] Applying these criteria, most ARSs appear to require a DPIA. Many ARSs will satisfy at least the following criteria: evaluation and scoring (including profiling), processing data concerning vulnerable data subjects, i.e. job applicants, and processing that may prevent job applicants from entering into an employment contract.[1073] Yet there is variation between ARSs. An ARS that evaluates job applicants based on their personal data clearly requires a DPIA,[1074] whereas one that merely transfers job applicants' personal data between systems may not.[1075]

Regarding innovative technology specifically, the EDPB has consistently held that this criterion alone does not require a DPIA,[1076] notwithstanding its explicit mention in GDPR Article 35(1) as likely to trigger a DPIA.[1077] However, where an additional criterion applies, such as the vulnerability of job applicants,[1078] a DPIA must be conducted.[1079]

Nevertheless, there may be ARS use cases where a DPIA is not required. For example, if a DPIA has been conducted for an earlier ARS, and a new ARS involves processing of a very similar nature, scope, context and purpose, a new DPIA would not be necessary in light of the WP29 guidance.[1080] A DPIA might not be required either if the processing falls within a national supervisory authority's optional exemption list under GDPR Article 35(5).[1081] Such DPIA-exempted lists have been

1072 The other criteria include conducting systematic monitoring, processing sensitive data or data of a highly personal nature, data processing on a large scale and matching or combining datasets. For a more detailed description of these situations, see (WP29 2017a, 9–11).

1073 (WP29 2017a, 9–11).

1074 See also (Dreyer and Schulz 2019, 10; Edwards and Veale 2017, 78).

1075 In line with the WP29 guidelines, the employers should then justify why a DPIA is not required and document these reasons (WP29 2017a, 12).

1076 See, e.g., (EDPB 2018c, 7–8; 2018d, 8; 2019c, 6).

1077 According to GDPR Recital 91, new technologies should be defined in 'accordance with the achieved state of technological knowledge'.

1078 In its guidelines on DPIA, the WP29 mentions, among other examples, employees as vulnerable data subjects, since, due to the power imbalance, they are unable to easily consent to, or oppose data processing, or utilise their rights. Yet, the WP29 acknowledges that vulnerability may exist 'in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified' (WP29 2017a, 10). As discussed in Section 1.1.1, job applicants are in an imbalanced position relative to the employer and may be more vulnerable than employees.

1079 See, e.g., (EDPB 2018c, 7–8; 2018d, 8; 2019c, 6).

1080 GDPR Art. 35(1) and (WP29 2017a, 12). Conversely, a new DPIA is required if the risks resulting from the ARS have changed, even if no new system is adopted (GDPR Art. 35(11)).

1081 GDPR Art. 35(5) and (WP29 2017a, 13).

drafted, for instance, by the supervisory authorities of Spain, France, Latvia and the Czech Republic. The exemptions applicable to employment relationships in the Czech, Latvian and Spanish lists do not appear to extend to job applicants who are not yet in an employment relationship.[1082] The French list, while including 'processing operations, implemented under the conditions laid down by the applicable texts, solely for human resources purposes' in sufficiently broad terms to potentially cover recruitment, restricts the exemption to employers with 'fewer than 250 people' and excludes profiling. [1083]

In any case, a DPIA serves not only as a duty but, as the WP29 has noted, as 'a process for building and demonstrating compliance' more broadly.[1084] Hence, to protect their own interests, employers may want to consider conducting an impact assessment even in cases where GDPR Article 35 or AIA Article 27 would not require it. The WP29 has also recommended conducting a DPIA in borderline cases to help ensure compliance with data protection law.[1085]

The GDPR sets minimum content requirements for a DPIA, though a meaningful assessment may demand considerably more than formal compliance with those requirements. Pursuant to GDPR Article 35(7), the DPIA should contain, at a minimum, a systematic description of the envisaged processing operations and purposes of the processing, an assessment of the processing operations' necessity and proportionality,[1086] an analysis of risks to rights and freedoms of data subjects[1087], and measures envisaged to address these risks (i.e. safeguards, security measures and mechanisms protecting personal data and assisting in demonstrating compliance).[1088] The WP29 guidelines on DPIA include a list of criteria for an acceptable DPIA.[1089] However, a proper assessment should go beyond a box-checking exercise to include a comprehensive analysis of what is done, how, why, what the consequences are, and how potential risks are mitigated. For instance, when conducted properly, the DPIA would assess how the employers' interests and needs in using the ARS have been balanced against its effects on job applicants' rights and the trade-offs made.[1090] The assessment must

1082 (Agencia Española Protección Datos 2019; Latvian Data State Inspectorate 2024; The Office for Personal Data Protection Czech Republic 2020).
1083 (CNIL 2019).
1084 (WP29 2017a, 4).
1085 (WP29 2017a, 8).
1086 This assessment could assist in evaluating the potential justifications for the use of ARSs that may disadvantage certain applicant groups.
1087 For an approach to assess the severity of impacts on fundamental rights, see (Malgieri and Santos 2025).
1088 GDPR Recital 90.
1089 See Annex 2 of the Guidelines, (WP29 2017a, 22).
1090 (Kelly-Lyth 2021, 915; ICO 2024, 30–31).

be documented, monitored and reviewed,[1091] meaning that the DPIA should be understood as a continuous process rather than a one-time compliance step.[1092] This ongoing character also means the DPIA can assist employers in meeting their duties under other legislation, such as assessing the ARS's potential discrimination risks.[1093]

Conducting the DPIA is the employer's responsibility, but it should not be undertaken in isolation.[1094] Rather, the employer should consult the stakeholders[1095] and 'where appropriate [...] seek the views of data subjects or their representatives on the intended processing'.[1096] Employers should therefore consider whether consulting job applicants is feasible. The WP29 has suggested, for instance, generic studies or questions to employee representatives as a means of seeking data subjects' views, and stated that refraining from consulting data subjects should be justified and documented.[1097] Although not mandatory, including ARS providers in the DPIA process could also prove highly useful for employers, since providers of high-risk AI systems must assess risks to fundamental rights, as part of their overall risk management systems under AIA Article 9.[1098] Furthermore, at least in cases of high-risk AI systems, the information provided under AIA Article 13 could assist in conducting the DPIA.[1099]

If the DPIA indicates that the residual risk remains high despite risk mitigation measures, the employer must consult the supervisory authority pursuant to GDPR

1091 (WP29 2017a, 16).

1092 (WP29 2017a, 14; Kosta 2020, 675).

1093 See also AIA Art. 27, which requires such employers that are public bodies or that provide public services to conduct fundamental rights impact assessments (FRIA), in which discrimination risks should also be covered. The FRIA will be discussed in some more detail below in this section. Frameworks to combine DPIA with AIA's FRIA requirements have also been proposed, see (Thomaidou and Limniotis 2025).

1094 GDPR Art. 35(2). See also (WP29 2017a, 14–15). As the WP29 notes, the DPIA may be carried out by someone else, but the responsibility for the DPIA lies with the controller.

1095 In addition to the employer as the controller, according to the WP29 guidelines these could include, for instance, the data protection officer, data subjects or their representatives, business, technical services, processors, and information security officer. See (WP29 2017a, 20).

1096 GDPR Art. 35(9). For instance, *Margot Kaminski and Gianclaudio Malgieri* have highlighted DPIA's collaborative role, see (Kaminski and Malgieri 2021, 131–32).

1097 (WP29 2017a, 15).

1098 Of the interplay of provider's risk assessment and deployer's impact assessment obligations in the context of the AIA, see also (Lasek-Markey and Hogan 2025, 4).

1099 See also AIA Art. 26(9). If the providers have conducted their own DPIAs on the systems, employers could benefit from accessing those. See also (WP29 2017a, 8).

Article 36 before using the ARS to process job applicants' personal data.[1100] The WP29 has clarified that consultation is required where the data controller cannot sufficiently address the identified risks, citing situations involving 'significant, or even irreversible, consequences, which [data subjects] may not overcome' such as a layoff and situations where 'it seems obvious that the risk will occur' such as 'when a well-known vulnerability is not patched'.[1101] The use of LLM-based recruitment systems, where confabulations cannot be reliably eliminated, may well fall within this category, given the potentially significant and irreversible consequences for job applicants. Yet, initially, the employers determine whether data protection authorities are consulted or not.[1102]

The prior consultation of data protection authorities under GDPR Article 36 appears to be the only ex-ante external oversight measure for ARSs.[1103] It affords data protection authorities the opportunity to intervene, even by prohibiting processing, if they consider that ARS use would infringe the GDPR.[1104] Consequently, the prior consultation procedure could incentivise employers to engage diligently with data protection considerations when adopting ARSs. However, the DPIA duty functions mainly as a procedural requirement shaping the process of ARS adoption and operation while facilitating the identification and mitigation of related risks.

Failure to comply with the DPIA duty may result in an administrative fine of up to 10 million euros or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[1105]

Specific duties for employers using AI systems

There is only one specific duty that concerns employers using any kind of AI recruitment system: the AI literacy duty set out in AIA Article 4. Accordingly, employers must ensure, to the best of their ability, that staff and other persons who operate and use AI systems on their behalf have a sufficient level of AI literacy.[1106] Under AIA Article 3, point 56, AI literacy comprises skills, knowledge and

1100 (WP29 2017a, 18–19).
1101 (WP29 2017a, 18–19).
1102 See section 6.1.1.4 below.
1103 Of DPIAs as ex-ante regulatory mechanisms, see also (Kosta 2020, 669).
1104 See GDPR Arts. 36(2) and 58.
1105 GDPR Art. 83(4).
1106 AIA Art. 4. AI literacy concerns both providers and deployers. When considering the sufficient level, the technical knowledge, experience, education, and training, as well as the AI system's context of use and the population for which it is intended, are to be noted. A sufficient level of literacy requires keeping pace with advancements. See also (Fernandes et al. 2024, 97).

understanding, allowing informed deployment of AI systems and awareness about the opportunities, risks and possible harms caused by AI. In practice, this means that staff should have both the required technical competence to use the system and the ability to handle the consequences of its use.[1107] Thus, AI literacy should enable informed decision-making regarding AI systems, allowing benefits from AI systems to be derived while protecting fundamental rights.[1108] Hence, AI literacy is increasingly important for the successful implementation of AI systems.

Regardless of its broad applicability, the AI literacy duty does not appear to impose a strong constraint on ARS use. It contains ambiguous and possibly restrictive wording, such as 'to their best extent' and 'sufficient level', leaving considerable discretion to the employer.[1109] Furthermore, its practical force is further limited by the absence of administrative fines for non-compliance.[1110] Nevertheless, unlike the high-risk obligations discussed next, the AI literacy duty is already in force as it became applicable 2nd February 2025.

Specific duties for employers using high-risk AI systems

Most of the AIA's duties assigned to deployers pertain only to deployers of *high-risk AI systems*. The obligations of high-risk AI system deployers are primarily set out in AIA Article 26, which specifically addresses the risks to safety and fundamental rights associated with the use of high-risk AI systems.[1111]

First, employers should implement appropriate technical and organisational measures to ensure compliance with the provider's instructions for using the high-risk AI recruitment system.[1112] These instructions may specify, for instance, the computational or hardware resources required to operate the system, as well as the maintenance and care measures required.[1113] Importantly, the instructions for use also determine the intended purpose of the AI system that employers should comply

[1107] (Fernandes et al. 2024, 95). The European Artificial Intelligence Office maintains a living repository of AI literacy practices to foster learning and the exchange of good practices, see (European Artificial Intelligence Office 2025).

[1108] AIA Recital 20. AIA Recital 91 further specifies that deployers must ensure that the persons responsible for implementing the instructions for use and human oversight must have an adequate level of AI literacy.

[1109] (Keller 2025, 146).

[1110] See AIA Art. 99. However, the breach of this duty could be considered as an aggravating factor if other breaches of the AIA are found and administrative fines based on those are imposed, see AIA Art. 99(7)(g).

[1111] AIA Recital 91. In prior scholarship, Art. 26 has been deemed to comprise an important part of the overall governance of high-risk AI systems' risks, see (Gallagher 2024, 541).

[1112] AIA Art. 26(1).

[1113] See AIA Art. 13(3)(e).

with.[1114] In case the employer utilises the high-risk AI recruitment system for purposes not intended initially and mentioned in the instructions for use, the employer may be considered a provider of the system based on AIA Article 25(1)(b).[1115] In practice, the instructions for use concretely shape the way the ARSs are used. However, there could be significant variations in the instructions as those are drafted by the providers without prior oversight.

Second, employers deploying high-risk AI systems must assign competent[1116], trained and authoritative persons to oversee the system, with the aim of preventing or minimising its risks.[1117] The provider's instructions for use should inform employers of the specific human oversight measures they must implement.[1118] The measures include appointing designated oversight personnel, providing additional training for those performing oversight tasks, and providing the required support for them.[1119] The feasibility of these duties, however, depends on the provider. If the provider has not designed the ARSs to include oversight features and sufficient transparency, including the provision of the information required by AIA Article 13, meaningful human oversight may, in practice, be impossible to implement.[1120]

Third, where input data is under the employer's control, it must be relevant and sufficiently representative considering the system's intended purpose.[1121] This duty supports data protection compliance, particularly with respect to the principles of data minimisation and accuracy. At the same time, the quality and representativeness of input data are also crucial for mitigating the risk of discrimination.[1122] Essentially, this duty gives explicit expression to what is already an implicit obligation under the

1114 AIA Art. 13(3)(b)(i). See also (Cristofolini 2024, 89).
1115 See also (Cefaliello and Kullmann 2022, 547).
1116 Based on AIA Recital 91, the competence appears to refer in particular to the adequate level of AI literacy. According to AIA Art. 14(4), the humans overseeing the system should properly understand the relevant capacities and limitations of the high-risk AI system and remain aware of automation bias. Moreover, humans should be able to 'duly monitor' the system's operation, including detecting and addressing anomalies, dysfunctions, and unexpected performance. The human overseers should be able to disregard, override or reverse the system's output and to intervene in its operation or interrupt the system safely.
1117 AIA Art. 14(2). However, human oversight is no panacea. *Alexia Gaudeul et al.* have found in a recent study that human oversight is insufficient to prevent discriminatory outcomes and may even make those worse (Gaudeul et al. 2024, 79).
1118 AIA Art. 13(3)(d). The providers have designed and developed these as required by AIA Art. 14.
1119 AIA Art. 26(2).
1120 It is the duty of the provider to develop the high-risk AI systems in a way that human oversight is possible, noting among others the requirements of AIA Art. 14(4).
1121 AIA Art. 26(4).
1122 (Gallagher 2024, 547).

Non-Discrimination Directives: the need to assess the representativeness of input data. Nevertheless, this duty does not in itself impose substantial additional constraints on ARS use.

Fourth, the AIA establishes several monitoring and reporting duties demanding employers to oversee high-risk AI recruitment systems throughout their operation.[1123] Employers must monitor system performance and operation in accordance with the provided instructions for use, with designated human oversight personnel carrying out these tasks.[1124] Furthermore, employers must report relevant performance information to the provider as part of the provider's post-market monitoring system. The scope of these duties is therefore partly dependent on the extent of the provider's post-market monitoring framework and the instructions for use.[1125]

Beyond routine monitoring, the AIA establishes reporting obligations triggered by identified risks or incidents. If an employer has reason to believe that using a high-risk AI system in accordance with its instructions could pose a risk to health, safety, or fundamental rights, they must inform the provider, distributor[1126], and the relevant market surveillance authority without undue delay.[1127] Upon identifying a serious incident[1128], employers must first immediately[1129] notify the provider, then the importer or distributor, and finally the market surveillance authorities. If the provider cannot be reached, the employer is responsible for informing the authorities in the same manner as the provider would under AIA Article 73.[1130] Meeting these reporting requirements demands clear internal policies and procedures, comparable

1123 See also (Cristofolini 2024, 91).

1124 AIA Arts. 26(5) and 14(4)(a).

1125 *Daniel Gallagher* has forecasted, based on the EU medical device regulation having similar post-market surveillance requirements, that post-market surveillance data could comprise, for example, user surveys, post-market follow-up studies, complaint systems, and focus groups (Gallagher 2024, 549).

1126 Pursuant to AIA Art. 3, point 7, a distributor refers to 'a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market'.

1127 See also AIA Arts. 26(5) and 79(1), Market Surveillance Regulation Art. 3, point 19. See also (Publication IV / Parviainen 2026).

1128 Under AIA Art. 3, point 49, a serious incident means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following: (a) person's death or serious harm to a person's health; (b) serious or irreversible disruption of the management or operation of critical infrastructure, (c) the infringement of EU fundamental rights obligations; or (d) serious harm to property or the environment.

1129 Commission's Draft Guidance on AIA Art. 73 regarding incident reporting suggests that the information should be provided within 24 hours (European Commission 2025e, 10).

1130 According to the Commission's Draft Guidance, the provider would be deemed unreachable if it does not answer within 24 hours (European Commission 2025e, 10).

to those already required under the GDPR.[1131] Employers must also cooperate with the relevant competent authorities in all actions related to the high-risk AI recruitment systems.[1132]

In terms of their practical effect on ARS use, the monitoring and reporting duties are primarily procedural, shaping how ARSs are operated rather than constraining what they may do. However, there is a notable exception: employers must suspend the use of systems that pose risks or have caused serious incidents.[1133] Nonetheless, the monitoring and reporting duties carry broader compliance benefits. Monitoring can assist employers in meeting their obligations under the Non-Discrimination Directives and the GDPR: if the monitoring reveals that the ARS is biased, the employer could prevent the biased outcomes from spreading. The reporting obligations, both towards providers and authorities, may similarly help prevent analogous problems from arising for potential other users of the same system.

Fifth, the providers must develop high-risk AI systems in a way that allows record-keeping.[1134] If the logs are under the employer's control,[1135] the employer must keep the logs automatically generated for an appropriate period, considering the intended purpose.[1136] If the logs contain personal data, the GDPR's principles of storage limitation and data minimisation should be considered when determining the retention periods. The records are designed to ensure traceability of the high-risk AI system's functioning, identify situations that pose risk, and facilitate the aforementioned post-market monitoring and evaluation of the system's operation.[1137] Hence, it would be in the interests of job applicants to keep the logs for a sufficiently long period to facilitate authorities' potential investigations.

Sixth, employers must inform workers' representatives and the affected workers that a high-risk AI system will be used in relation to them.[1138] Since workers may also be applying for other positions within the same organisation, this obligation

1131 (Gallagher 2024, 549). As the GDPR's reporting duties are general and do not specifically constrain ARS use, those were not included in the framework of key legal parameters.

1132 AIA Art. 26(12). Since this does not require any proactive measures from the deployers, it is not included as a separate duty in the categorisation.

1133 AIA Art. 26(5). Regarding systems that cause serious incidents, this duty is not explicitly mentioned in the article; however, it follows logically that such systems must also be considered risky, as the incident demonstrates that the risks have already materialised.

1134 AIA Art. 12(2).

1135 (Gallagher 2024, 547) has pointed out that this is likely the case if the AI system is deployed on the deployer's infrastructure, and less so when AI is acquired as-a-service.

1136 AIA Art. 26(6). The period shall be at least six months, unless provided otherwise in applicable EU or national law.

1137 AIA Art. 12(2).

1138 AIA Art. 26(7). Of the value of this right to job applicants, see section 6.1.2 below.

extends to the introduction of high-risk AI recruitment systems. The AIA does not specify the exact content of the information to be provided nor the procedures. Accordingly, national information and consultation obligations play a key role in concretising this duty.[1139] The national procedures may also entitle employee representatives to request additional details, creating an important opportunity for further dialogue and clarification. However, this obligation applies only to existing employees and their representatives and therefore offers little direct benefit to external job applicants.[1140]

If an employer provides public services, it must also carry out a fundamental rights impact assessment (FRIA).[1141] The FRIA shares notable similarities with DPIAs.[1142] To remove redundancies, the FRIA may be conducted as part of the DPIA process.[1143] However, while the DPIA focuses primarily on data protection, the FRIA requires broader consideration of all potentially affected fundamental rights and freedoms.[1144] According to AIA Recital 48, certain fundamental rights are of particular importance and should receive special attention.[1145] Hence, conducting only a basic DPIA would usually not be sufficient to fulfil the FRIA duty.

Under AIA Article 27(1), the FRIA must comprise, among other issues, the assessment of the processes in which the system is used and when, the categories of persons or groups likely to be affected, the specific risks of harm, human oversight measures and measures to be taken in case the risks materialise.[1146] Similar to the

[1139] The information obligations under the AIA do not override potential national information and consultation obligations, but rather complement those requirements. See AIA Art. 2(11).

[1140] In many cases the job applicants would, nevertheless, be entitled to information under AIA Art. 26(11) as discussed below.

[1141] AIA Art. 27 and Recital 96. See also (Mantelero 2024).

[1142] (Mantelero 2024, 4; Fülop and Poindl 2024, 571–73).

[1143] (Thomaidou and Limniotis 2025).

[1144] (Mantelero 2024, 4). *Tünde Fülop* and *Philipp Poindl* emphasise that while certain fundamental rights might be at greater risk than others, AI systems might impact all fundamental rights (Fülop and Poindl 2024, 562).

[1145] These include 'the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, the right to education, consumer protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, and the right to good administration.' Children's rights and the right to a high level of environmental protection are also specifically noted.

[1146] See also (Fülop and Poindl 2024, 568–71).

DPIA, the FRIA must be completed before the AI recruitment system is used and should be updated where necessary.[1147]

The AIA also imposes duties on deployers that are triggered only when *the high-risk AI system assists in individual decision-making*. Namely, the employers have a duty to inform job applicants that a high-risk AI system is assisting or making decisions related to them.[1148] This obligation also applies to situations where the high-risk AI recruitment system merely assists in decision-making.[1149] The information to be provided should include disclosure of the use of high-risk AI in decision-making, its intended purpose, the type of decisions to be made, and information about the job applicants' right to an explanation under AIA.[1150] However, AIA Article 26(11) does not require the provision of details regarding the ARS or its effects.[1151]

In practice, complying with the employers' duties under the AIA necessitates establishing governance, monitoring, and reporting policies and procedures, as well as contractual arrangements that enable employers to fulfil their duties.[1152] Nevertheless, many of the employers' duties under the AIA cannot be effectively fulfilled unless the provider has also met its own responsibilities under the AIA. In many respects, employers' duties are shaped by the provider's instructions for use, such as in the areas of human oversight, monitoring, and reporting. The high-risk AI system deployers' duties are therefore closely intertwined with those imposed on the systems themselves, which providers are ultimately responsible for. While employers' duties primarily influence the organisation's recruitment processes, the provider's obligations and the technical and compliance requirements placed on high-risk AI recruitment systems play a decisive role in shaping and limiting the functioning of these systems.[1153]

Unlike the AI literacy obligation, breaches of the high-risk AI system deployers' duties are subject to administrative fines under AIA Article 99(4). Non-compliance with the duties could lead to administrative fines of up to 15 million euros or 3 % of undertakings' total worldwide annual turnover for the preceding financial year,

1147 AIA Art. 27(1). Further, the same FRIA can be relied on in similar cases. AIA Art. 27(2) also explicitly allows the deployer to rely on the provider's existing impact assessment.
1148 AIA Art. 26(11).
1149 Cf. GDPR Arts. 13(2)(f) and 14(2)(g).
1150 See AIA Recital 93.
1151 Cf. GDPR Arts. 13(2)(f) and 14(2)(g).
1152 (Gallagher 2024, 544 and 550–51). If the employer delegates the use of the ARS to a recruitment agency, contractual arrangements should also be in place.
1153 See, e.g. (Cristofolini 2024, 86).

whichever is higher.[1154] The market surveillance authorities responsible for overseeing compliance with the AIA exercise the powers granted to them under the Market Surveillance Regulation, as further supplemented by the AIA.[1155] Hence, these authorities may, for instance, conduct unannounced on-site inspections or physical checks of AI recruitment systems[1156] and order the cessation of non-compliant practices.[1157]

Specific duties related to ADM

Before conducting ADM,[1158] the employers are obliged to inform job applicants under GDPR Articles 13(2)(f) or 14(2)(g) of the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. It was long unclear and debated by the legal scholars what these provisions entail in practice.[1159]

The CJEU judgment in *Dun & Bradstreet Austria* casts some light on what 'meaningful information about the logic involved' requires. The CJEU suggested that the meaningfulness of the information could refer both to the good intelligibility and value of the information.[1160] Further, it considered that the logic involved comprises 'the procedure and principles relating to the use, by automated means, of personal data with a view to obtaining a specific result'.[1161] In an algorithmic

[1154] If some breach could amount to breaching both the GDPR and the AIA, such as not informing the job applicants of using ARS for automated decision-making, the sanctions for the breach under the GDPR could be higher (see GDPR Arts. 83(5) and section 5.2.2 above).

[1155] See, e.g., AIA Art. 74.

[1156] Art. 14(4)(d) of the Market Surveillance Regulation.

[1157] Art. 14(4)(g) of the Market Surveillance Regulation.

[1158] When the personal data is collected from the applicant, the information must be provided at the time when personal data are obtained (GDPR Art. 13(1)). Instead, when the personal data have been obtained from other sources, the information shall be provided (a) within a reasonable period after obtaining the data (max within one month), (b) at the latest when first communication to the data subject if the data is used for such purposes and (c) at the latest when the personal data are first disclosed to another recipient (GDPR Art. 14(3)), unless exceptions listed in GDPR Art. 14(5) apply.

[1159] See, e.g., (Wachter et al. 2017, 76, 78 and 82–83; Grozdanovski 2021, 123–24; WP29 2018a, 25–26; Vedder and Naudts 2017, 215; Brkan 2019a, 110–19). The WP29 guidelines provided some interpretative assistance (WP29 2018a, 24–26), which the CJEU has also noted in its judgment C-203/22 *Dun & Bradstreet Austria* (explicitly in paras 45 and 60).

[1160] See C-203/22 *Dun & Bradstreet Austria*, paras 40–41.

[1161] See C-203/22 *Dun & Bradstreet Austria*, paras 43.

recruitment context, that could mean, for instance, disclosing the type of personal data used, the criteria considered in decision-making and their weights on an aggregate level.[1162] The information should be provided to job applicants in a manner that an average job applicant can understand, and so that they can utilise the information to enforce their other rights under the GDPR.[1163] The WP29 guidelines on transparency propose that the level of intelligibility, transparency and effectiveness of the information and user interfaces could be tested through various mechanisms to ensure that they are understandable for the audience, in this case, the job applicants.[1164]

This duty to inform job applicants could enhance transparency in algorithmic recruitment processes. However, the CJEU's interpretation of the provisions does not seem to require very detailed information disclosures, making it possible to comply with this obligation also if the ARS is not fully interpretable.[1165] Hence, this duty does not significantly constrain ARS use, but rather again shapes the usage procedure.

5.2.4 Actionable rights

Job applicants' actionable rights are treated as a distinct category within the framework of key legal parameters for ARS use since, unlike the parameters in the categories discussed above, these legal parameters require job applicants to actively invoke them to take effect.[1166] Identifying actionable rights as a separate category also serves a practical purpose: it provides an overview of the rights available to job applicants when ARSs are used, helping them navigate the legal framework more effectively.

Although framed as actionable, this category of legal parameters is not reduced to purely reactive protections. Employers must ensure that these rights can be fulfilled even before any individual seeks to exercise them. For example, employers must be able to provide applicants with explanations when ADM or AI-assisted decision-making is used. These rights should therefore be acknowledged and enabled

1162 See also AG Pikamäe's opinion in C-634/21 *Schufa* paras 54-58.

1163 See C-203/22 *Dun & Bradstreet Austria*, para 58. Of the assumed focus on average or lay data subjects' view, see (Metikoš 2025; WP29 2018c, 7).

1164 (WP29 2018c, 7). The means suggested by the WP29 include user panels, readability testing, interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies.

1165 (Metikoš 2025; Rosin and Parviainen 2025, 488).

1166 See GDPR Arts. 12–14. Rights to transparency that do not require any proactivity on the job applicants' side have been included in the obligations section 5.2.2, and, as regards ADM, in section 5.2.3. See also section 6.1.2 below.

by default, with the result that they may directly shape the design and operation of ARSs.[1167]

Actionable rights concerning all ARSs

The right of access enshrined in Article 8 of the CFREU and specified in Article 15 of the GDPR is a cornerstone of job applicants' rights.[1168] The CJEU and the EDPB have highlighted the importance of this right in enabling data subjects to verify the lawfulness of processing and the accuracy of the processed data.[1169] It is also crucial to ensuring that job applicants can effectively exercise their other rights and contest ARSs.[1170]

When job applicants exercise their right of access, employers should inform applicants whether their personal data is processed, provide access to that data, and provide information about its processing and data subjects' rights.[1171] Moreover, job applicants can request a copy of their personal data.[1172]

The EDPB has stated that the right of access covers several types of personal data, including data knowingly and actively provided by the data subject, observed data or raw data provided by the data subject by using the service, data derived from other data and data inferred from other data.[1173] Thus, it is clear that the right of access also covers various personal data created by the ARS or the employer.[1174] For instance, a summary of the CV and application drafted by an LLM-based recruitment system, or a profile inferred from those, would be an applicant's personal data created during the recruitment process and to which they must be granted access.[1175]

The EDPB has highlighted that the information on the processing and the personal data processed should reflect the situation at the time when the data subject

[1167] See also GDPR Art. 25.
[1168] Of the importance of this right, see also (Ausloos and Dewitte 2018, 4 and 7).
[1169] C-487/21 *CRIF*, paras 34 and 35 and C-154/21 *Österreichische Post*, paras 37–38. (EDPB 2023, 8 and 10). See also GDPR Recital 63.
[1170] See, e.g., C-579/21 *Pankki S*, para 83 and C-203/22 *Dun & Bradstreet Austria*, paras 53 and 55-56. See also (EDPB 2023, 3 and 9). Of the importance of this right to job applicants as an informational safeguard, see also section 6.1.2 below.
[1171] GDPR Art. 15(1) and (2). The EDPB has pointed out that the information to be provided under the right of access should be updated and tailored so that it actually corresponds to the processing operations carried out on the requesting data subject's personal data (EDPB 2023, 37–38).
[1172] GDPR Art. 15(3). See also (EDPB 2023, 13).
[1173] (EDPB 2023, 32–33).
[1174] (Custers and Vrabec 2024, 8; EDPB 2023, 33). Based on case C-597/21 *Pankki S*, the right appears to also cover log data. Similarly, also in (EDPB 2023, 32–33).
[1175] See also (EDPB 2023, 32–33).

makes the access request.[1176] Accordingly, exercising the right of access after decisions are made enables job applicants to become aware of the decisions and profiles created about them, which is crucial to analysing their lawfulness and challenging them.[1177] As the EDPB has pointed out, becoming aware of the 'unlawful processing concerning the data subject is one of the main purposes of the right of access'.[1178] Consequently, the EDPB has stated that if controllers detect inaccurate data or unlawful processing when handling an access request, they should first inform the data subject of those issues and the planned corrective measures before taking any corrective action.[1179] However, the right of access is not unconditional.

GDPR Article 15(4) allows employers to potentially withhold certain information if providing a copy of the personal data would adversely affect the rights and freedoms of others. According to GDPR Recital 63, the rights and freedoms of others could be, for instance, trade secrets, intellectual property or copyright.[1180] The EDPB has emphasised that a company's economic interests not to disclose personal data alone would not suffice to allow exemptions to the right of access.[1181] Based on GDPR Recital 63, the consideration of others' rights and freedoms should not lead to refraining from providing all information to data subjects.[1182] In practice, this could lead to difficult balancing situations that employers should initially resolve.[1183] If the applicant contests the employer's decision to refrain from providing their personal data, the employer must provide the allegedly protected information to a supervisory authority or court upon demand, which will then balance the rights and interests and determine to what extent the job applicant should be granted access.[1184]

1176 (EDPB 2023, 18).

1177 C-203/22 *Dun & Bradstreet Austria,* paras 53 and 55–56. See also (WP29 2018a, 27). In the context of ADM, the right of access is also deemed to constitute a right to explanation, see case C-203/22 *Dun & Bradstreet Austria*, para 57. For more detailed information, see section 5.2.4 below on actionable rights related to ADM.

1178 (EDPB 2023, 18).

1179 (EDPB 2023, 19).

1180 See also cases C-487/21 *Österreichische Datenschutzbehörde and CRIF*, para 43 and C-203/22 *Dun & Bradstreet Austria*, para 71. Under GDPR Article 23, also EU or Member State law may further restrict the right of access.

1181 (EDPB 2023, 52–53).

1182 GDPR Recital 63 and C-203/22 *Dun & Bradstreet Austria*, para 72. See also (EDPB 2023, 52).

1183 For instance, *Bart Custers and Anne-Sophie Heijne* have suggested that, to better balance the competing interests, access requests should be addressed on a rather personalised basis, considering the principles of proportionality and necessity (Custers and Heijne 2022, 15).

1184 C-203/22 *Dun & Bradstreet Austria,* para 76.

The right of access requires controllers to be proactively ready to handle the access requests.[1185] Thus, employers should ensure that the ARS allows easy access to personal data and that internal procedures are in place to facilitate the fulfilment of this right.[1186] The complexity of the ARSs and the potential obscurity of their processing operations make compliance more difficult than in traditional software systems, as locating and collating all job applicants' personal data in a way that is intelligible to them, as required by GDPR Article 12(1), may require dedicated technical and procedural measures that employers must anticipate.

If job applicants identify incorrect information in their personal data, they have the right to rectification under GDPR Article 16, which requires inaccurate personal data to be rectified and incomplete personal data to be completed.[1187] Beyond the 'raw' personal data collected by the ARS, the WP29 has considered that the right to rectification should also encompass any profile or score derived from such data.[1188] The scope of the right becomes less straightforward, however, when applied to inferences. It can be challenging to determine both when inferences are incorrect and require rectification and whether they are used for purposes to which the right applies in the first place. For example, the CJEU has considered that the right to rectification does not extend to test results.[1189] By analogy, it could be argued that the right to rectification does not apply to the decisions regarding job applicants' suitability, as extending the right to such decisions would undermine their purpose. Practical complications also arise at the technical level.[1190] Although rectifying the profiles generated by ARSs could possibly be done manually, the difficulty increases considerably if personal data is embedded in the ARS's model.[1191] Allegedly, rectifying personal data from the ARS's model is a formidable task.[1192]

Pursuant to GDPR Article 17, job applicants have also a right to erasure of their personal data in some more limited situations where, for instance, personal data is no longer necessary for the recruitment purposes, there are no legal grounds for processing, the job applicant has objected to the processing and no overriding legitimate grounds for processing exist, the processing has been unlawful or there is a legal obligation to erase the data. However, this right is not without limitations,

1185 (EDPB 2023, 20).
1186 See GDPR Art. 12(2).
1187 GDPR Art. 16.
1188 (WP29 2018a, 17). See also (Custers and Vrabec 2024, 9).
1189 C-434/16 *Nowak*, para 53. See also (Wachter and Mittelstadt 2019, 538–39, 550; Dimitrova 2020, 219–21).
1190 (Custers and Vrabec 2024, 10). *Bart Custers and Helena Vrabec* have considered that controllers are not required to include the corrections in the subsequent analysis, which would reduce the effects of this right.
1191 (Veale et al. 2018, 8).
1192 Of the possibilities of machine unlearning in such cases, see (Novelli et al. 2024, 9).

and the personal data could be retained despite job applicants' requests, for example, if it is necessary for the establishment, exercise or defence of legal claims.[1193] The right to erasure applies to both the input personal data (e.g. provided in the job application, or through tests) and the output data (e.g. a profile generated or a decision made).[1194] Again, if the personal data is part of the ARS's model, complying with the right to erasure could be problematic.[1195] Thus, both the right to rectification and the right to erasure may constrain the use of ARS models that include personal data, as employers should ensure compliance with job applicants' rights even before those rights are invoked.

Under GDPR Article 18, job applicants can also request restrictions on the processing of their personal data in specific situations where they have used their rights by contesting the accuracy of the decisions[1196] or objected to the processing[1197], but the controller's actions are pending. Additionally, restrictions on processing could be relied on where processing is unlawful[1198] or no longer necessary,[1199] but job applicants resist erasure, for instance, to initiate legal claims against the employer. Restriction of processing requires technical means in the systems to ensure that personal data is no longer processed or changed.[1200] When processing is restricted, personal data may only be stored or used in legal claims. Other processing requires job applicants' consent.[1201] As long as the personal data is not fed into the ARS in the use phase in a way that it would become a part of the model, this right does not constrain ARSs use. Rather, the right to restrict processing sets technical requirements which any software that processes job applicants' data should fulfil.

1193 GDPR Art. 17(3). For instance, the Finnish DPA has considered in a decision given on 13.8.2020 (No. 6652/154/19) that, as the period for bringing charges for work discrimination within the meaning of Chapter 47, Section 3 of the Finnish Criminal Code (39/1889) was two years, the controller could lawfully refuse the request to erase a job applicant's personal data during the two-year period. Yet, the period for bringing charges also appeared to set the maximum period for processing personal data. At the end of that period, the controller should know whether charges have been raised. If not, there is no need to store the job applicants' personal data further.

1194 (WP29 2018a, 18).

1195 See, e.g., (Edwards and Veale 2017, 69–71; Wachter and Mittelstadt 2019, 599; Villaronga et al. 2018, 307–10). *Custers and Vrabec* have also emphasised the problems of erasure with inferred data, see (Custers and Vrabec 2024, 10).

1196 GDPR Art. 18(1)(a).

1197 GDPR Art. 18(1)(d).

1198 GDPR Art. 18(1)(b).

1199 GDPR Art. 18(1)(c).

1200 GDPR Recital 67.

1201 GDPR Art. 18(2).

Furthermore, the right to data portability established in GDPR Article 20 complements the right of access by giving job applicants the right to receive their personal data they have provided to the employer in 'a structured, commonly used and machine-readable format'.[1202] Another part of the right to data portability is job applicants' right to transmit their data to another employer.[1203] However, this right applies only where the processing is based on the job applicants' consent or contract.[1204] The WP29 guidelines suggest that the right to data portability cover both the 'raw' personal data provided by the applicants and the personal data generated by and collected from their interactions with the ARS. Yet, unlike the right of access, it would not cover data that are exclusively generated by the employer, e.g. profiles on their employability.[1205] The data portability right could establish technical requirements for the ARSs to be considered when building or acquiring the systems, but it does not constrain their use.

Finally, to the extent that processing is based on legitimate interests,[1206] job applicants may object to the processing of their personal data[1207] on grounds relating to their particular situation.[1208] As the GDPR does not specify what the particular situation could comprise, the concept remains somewhat ambiguous. The WP29 has suggested that the data subject's particular situation could refer to personal, social or professional reasons.[1209] Since the legitimate interests must be weighed against the data subject's particular situation, the objection must articulate the grounds relied upon.[1210]

Namely, GDPR Article 21(1) permits continued processing despite objections where there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. Where a job applicant has raised an objection, the

1202 GDPR Recital 68 adds that the data should also be provided in an interoperable format. See also (WP29 2016, 4–5).
1203 (WP29 2016, 5).
1204 GDPR Art. 20(1).
1205 See (WP29 2016, 8).
1206 GDPR Art. 21(1) allows the right to object to be utilised also when processing is necessary for the performance of public interest tasks or the exercise of official authority, but these are not triggered in private sector recruitment.
1207 GDPR Art. 21(1) expressly mentions profiling as an example of processing to which the right to object extends. However, it is not limited only to profiling but covers all processing.
1208 GDPR Art. 21(1). See also (EDPB 2024a, 21–22).
1209 (WP29 2018a, 19). Possibly, job applicants' suspicion of being discriminated against by the system might be a sufficient situation to uphold the objection.
1210 While not explicitly stated in the EDPB guidelines, those also note the possibility to ask data subjects to further specify the requests if there are doubts about the particular situation (EDPB 2024a, 21–22).

employer must conduct a new balancing test to assess whether its compelling legitimate grounds take precedence over the job applicant's rights, freedoms and interests in the particular situation so that it may continue processing despite the objection.[1211] The EDPB has emphasised that, at this stage, the grounds to justify processing should be even higher than those in the initial balancing test required under GDPR Article 6(1)(f).[1212] According to the EDPB, the compelling grounds should be 'essential to the controller', such as where processing of personal data is required to protect systems from immediate harm or the organisation from a severe business-affecting penalty.[1213] In prior scholarship, for instance, *Marta Otto* has assumed that an employer's mere commercial interest in using a prehiring algorithm would not constitute a compelling legitimate interest when job applicants' rights to privacy and data protection are interfered with.[1214] *Aislinn Kelly-Lyth* has suggested that, although unlikely, compelling legitimate grounds might exceptionally exist if the ARS has increased the diversity of hiring, as it *might* be beneficial for society at large and therefore justified in light of WP29 guidance on ADM.[1215] Yet, while the benefit for society could legitimate the use of ARSs in general, it is less likely to override the individual applicants' objections. If no compelling legitimate grounds can be demonstrated, the employer must stop processing personal data as requested.[1216]

Consequently, if the processing of personal data relies on legitimate interests, employers must be prepared to either demonstrate compelling legitimate grounds for processing or to manage the recruitment process manually in a non-discriminatory manner, even if some job applicants object to certain processing activities. Job applicants might object only to profiling or automated decision-making, as objecting to all processing of their personal data would make proceeding in the recruitment process practically impossible. When utilised, the right to object could, in individual cases, constrain the use of ARSs.

The sanctions for failing to uphold these rights are similar to those applicable to breaches of general obligations under the GDPR, underscoring the seriousness with which these rights should be treated.[1217]

1211 (EDPB 2024a, 21–22).
1212 (EDPB 2024a, 21–22).
1213 (EDPB 2024a, 21–22).
1214 (Otto 2018, 397). C-131/12 *Google Spain*, para 97.
1215 (Kelly-Lyth 2021, 910; WP29 2018a, 18). WP29 provides profiling to predict the spread of contagious diseases as an example of societal benefit.
1216 See also (Otto 2018, 397).
1217 See section 5.3.2 above.

Actionable rights related to high-risk AI systems assisting decision-making

Under AIA Article 86, job applicants have a right to an explanation of individual decision-making, when employer takes a decision 'on the basis of the output from a high-risk AI system' and when the decision 'produces legal effects or similarly significantly affects' the job applicant 'in a way that they consider to have an adverse impact on their health, safety or fundamental rights'. Importantly, the AIA's right to an explanation extends to decisions that humans take based on an AI system's output, and not only to fully automated decisions.[1218] However, when the decision does not have legal effects, the right is triggered only if the job applicant considers that the decision has similarly significant *adverse* effects on them.[1219] Under these circumstances, employers using high-risk AI recruitment systems must provide information about the decision-making to job applicants upon request.

The explanation provided to job applicants should be clear and meaningful, covering 'the role of the AI system in the decision-making procedure and the main elements of the decision taken'.[1220] According to AIA Recital 171, the explanations should enable affected persons to exercise their rights. The role of the AI system could be explained by outlining the parts of the recruitment process which the ARS manages and specifying the extent of human recruiters' involvement.[1221] However, the requirement to disclose 'the main elements of the decision taken' is more ambiguous.[1222] *Maja Brkan* and *Hana Palčič Vilfan* have proposed that those elements could include details on 'the types of algorithms used for processing data and their underlying logic (determining the weights of and relationships among data), the input data and training data used, the model's output, the probabilities, the decision-making criteria used'.[1223]

[1218] Cf. GDPR Art. 22(1). For the relationship between AIA Art. 86 and GDPR Art. 15(1)(h) see (Publication IV / Parviainen 2026), (Rosin and Parviainen 2025, 488–89) and section 6.1.2.2 below. See also (Brkan and Palčič Vilfan 2024, 1203–4; Grozdanovski 2025).

[1219] The job applicants themselves are to decide when the adversity threshold is met initially. Cf. GDPR's right to explanation applies when the automated decision has legal or similarly significant effects, and it does not explicitly require adverse effects (see GDPR Arts. 22(1) and 15(1)(h)). See also (Publication IV / Parviainen 2026), where it has been stated that from the point of view of an individual applicant, AIA's limitation is understandable, as remedies are needed less often in positive decisions. However, when considering the job applicants as a group, they could also require information about the positive decisions to build their claims against discriminatory ARSs.

[1220] AIA Art. 86(1).

[1221] (Carter 2024, 356).

[1222] This point was changed during the legislative process, and there could be different ways to interpret it, as *Christine Carter* has pointed out (Carter 2024, 356).

[1223] (Brkan and Palčič Vilfan 2024, 1207).

To ensure that job applicants can meaningfully exercise their rights, employers should provide explanations that allow job applicants to interpret the AI recruitment system's output and comprehend the rationale behind it.[1224] While an in-depth technical explanation of the system's inner workings is not likely required,[1225] the explanation should at least address the key factors that influenced the decision.[1226] Thus, the requirement to explain 'the main elements of the decision taken' may align relatively closely with the obligation to explain the logic involved under the GDPR.[1227]

Nonetheless, employers may not always be well-equipped to provide explanations, as they are also likely to struggle to understand the ARS's workings and hence be reliant on the information the ARS provider gives them under AIA Article 13. Employers must ensure that they sufficiently understand the system's operation and, if necessary, seek additional information from the provider.[1228] To ensure compliance with this obligation, employers should proactively anticipate the need for explanations and prepare to provide them in advance.

AIA Article 86(3) specifies that the right to an explanation applies only in situations where EU law does not already mandate the provision of explanations.[1229] Following the CJEU judgment in *Dun & Bradstreet Austria*, the GDPR may be interpreted as creating a right to an explanation in cases where ADM is used, as will be discussed below. In instances of ADM, the GDPR's right takes precedence, whereas in other cases, the AIA's right could be invoked. Since AI-assisted decision-making may be even more prevalent than ADM in recruitment,[1230] the AIA's right to an explanation could be invoked more frequently.

Non-compliance with the job applicants' right to explanation under the AIA is not related to a direct threat of fines, compensation or damages under the AIA.[1231]

1224 See also (Cristofolini 2024, 93 and 95) .

1225 (Hacker 2024a, 11–12).

1226 (Carter 2024, 356). *Christine Carter* has suggested that the main elements of the decision taken could include, for instance, 'access to data indicating how bias emerged in training data, label and feature selection'.

1227 See also C-203/22 *Dun & Bradstreet Austria*, para 58. The WP29, in its good practice recommendations, noted that meaningful information about the logic involved could include, for instance, the categories of data used in the decision-making process, why those were important, how profiles were built, and how the profiles were used to reach a decision (WP29 2018a, 31). See also (Metikoš and Ausloos 2025, 229).

1228 See also (Demkova 2024; Nisevic et al. 2024, 5 and 7).

1229 For a discussion on this requirement, see (Publication IV / Parviainen 2026).

1230 See, e.g., (ICO 2024, 32).

1231 AIA Art. 99 does not include a fine for breaching AIA Art. 86. See also (Nnawuchi and George 2024, 409–10) and (Publication IV / Parviainen 2026).

Actionable rights related to ADM

The GDPR provides several actionable rights related to ADM.[1232] As mentioned, the CJEU has now settled the heated academic debate on whether the GDPR provides a right to explanation of automated decision-making, ruling that such a right exists. In *Dun & Bradstreet Austria,* the CJEU stated that the meaningful information about the logic involved to be disclosed based on GDPR Article 15(1)(h) 'must be understood as a right to an explanation of the procedure and principles actually applied' in automated decision-making.[1233] The CJEU considered that to enable data subjects to effectively exercise the rights conferred on them by the GDPR, particularly Article 22(3),[1234] the explanation must contain relevant information and be in a concise, transparent, intelligible and easily accessible form.[1235]

As noted in the WP29 guidelines on transparency, there is an inherent tension between the comprehensive information that is required to be provided and its conciseness, transparency, intelligibility and accessibility.[1236] This tension is also present in the context of explanations. On the one hand, the CJEU acknowledges that the aim of the explanation is to facilitate the exercise of data subjects' rights.[1237] In practice, exercising the right to challenge the decision, at least in court, could require detailed and technical information about the processing if the unlawfulness is not clearly visible from the explanation, which is unlikely.[1238] On the other hand, the information must be concise, transparent and intelligible,[1239] which the information needed to challenge the decisions may not be for average data subjects. When balancing these aims, the CJEU appears to emphasise the usability and meaningfulness of the information to the individual data subject at the cost of informativeness. According to the CJEU, the explanation should enable data subjects to understand which of their personal data has been used in the decision-making and confirm its accuracy.[1240] For instance, disclosing the algorithm used would not be sufficiently concise and

1232 These are discussed in more detail from the perspective of the job applicants in section 6.1.3.1 below.
1233 C-203/22 *Dun & Bradstreet Austria*, para 58.
1234 The importance of being informed about ADM as a prerequisite for utilising the safeguards has also been emphasised by the WP29 and scholars, see (WP29 2018a, 27; Malgieri 2019, 9–10).
1235 C-203/22 *Dun & Bradstreet Austria,* para 58. See also GDPR Art. 12(1).
1236 (WP29 2018c, 18).
1237 C-203/22 *Dun & Bradstreet Austria*, para 58.
1238 See also (Metikoš 2025).
1239 C-203/22 *Dun & Bradstreet Austria*, para 58.
1240 C-203/22 *Dun & Bradstreet Austria*, paras 61 and 63.

intelligible.[1241] Instead, the CJEU has considered that informing data subjects about counterfactuals[1242], that is how variations in their personal data could have led to an alternative outcome, could be a sufficiently transparent and intelligible explanation.[1243] Yet, the usefulness of counterfactuals in contestations remains debatable.[1244]

Consequently, the right to explanation as interpreted by the CJEU does not appear to require that all the details of the ARSs are explainable. Instead, simplified descriptions of the procedure and principles actually applied could be sufficient.[1245] Therefore, the right to explanation, as the CJEU has so far interpreted it, does not seem to constrain the use of complex and intractable ARSs, as long as their logic can be explained to average job applicants in a way that enables job applicants to exercise their rights, especially under GDPR Article 22(3).[1246]

When ADM is involved, GDPR Article 22(3) grants job applicants the interconnected rights to request human intervention, express their viewpoints on the automated decisions[1247] and challenge those decisions. WP29 has emphasised that a simple way to exercise these rights must be provided.[1248] While it is possible to request human intervention without prior explanations, the ability to meaningfully articulate viewpoints or challenge decisions clearly depends on having access to an adequate explanation of the decision-making process.[1249] Beyond granting applicants the opportunity to challenge automated decisions, these procedural safeguards can also be understood as means of quality control within the recruitment process.[1250]

Human intervention might be realised, for instance, by providing a link to an appeal process at the time when the job applicant is informed of the decision.[1251]

1241 C-203/22 *Dun & Bradstreet Austria*, para 58. The WP29 guidelines also suggested that disclosing the algorithm would not be needed (WP29 2018a, 25) and that the information should be intelligible for 'an average member of the intended audience' (WP29 2018c, 7) and thus not utilise 'overly legalistic, technical or specialist language or terminology' (WP29 2018c, 10).

1242 See, e.g., (Wachter et al. 2018, 844–46).

1243 C-203/22 *Dun & Bradstreet Austria*, para 62.

1244 In favour of counterfactuals, see, e.g., (Wachter et al. 2018). Cf. more sceptical of counterfactuals, see, e.g., (Barocas et al. 2020; Metikoš 2025).

1245 (Rosin and Parviainen 2025, 488; Metikoš 2025).

1246 The WP29 has suggested that challenging a decision and expressing one's view require a full understanding of how the decision was made and on what basis (WP29 2018a, 27).

1247 (Malgieri 2019, 22). Cf. Some have argued that the opinion on automated decision-making should be allowed to be expressed at any stage, including prior to the issuance of final decisions. See (Kamarinou et al. 2016, 4–5).

1248 (WP29 2018a, 27).

1249 Of the need for transparency about the processing when exercising these rights, see also (WP29 2018a, 27).

1250 (Mendoza and Bygrave 2017, 7; Almada 2019, 2–3; Dreyer and Schulz 2019, 43).

1251 (WP29 2018a, 32).

Moreover, as instructed by the WP29, the employer must ascertain that the human(s) intervening possess the appropriate authority and capability to make or modify the decision.[1252] The human should conduct a thorough assessment of the relevant data, including potential additional data provided by the applicant.[1253] Job applicants could also express their point of view, either separately or in conjunction with a request for human intervention, provided they have been given sufficient information about the decision-making process to form an informed opinion.[1254]

Finally, job applicants must be provided an opportunity to contest automated decisions. Yet, the specifics of this process are left open in the GDPR. Based on WP29 guidance, in practice, the right to contest the automated decision requires that some way to challenge the decision is offered to job applicants, such as a form in the ARS.[1255] The grounds for contesting are not specified in the GDPR, allowing job applicants to contest decisions on various grounds. Neither does the GDPR establish substantive standards for evaluating the decision itself, which could complicate the handling of the complaints.[1256] While GDPR Article 22(3) does not expressly state that a human should handle the appeal, when read together with the other minimum safeguards, the provision could be deemed to require that, at least when the applicant so requests, a human should process the complaints.[1257]

Consequently, the safeguards clearly shape the design of the algorithmic recruitment process when ADM is employed, but do not significantly constrain ARS use.

[1252] (WP29 2018a, 27; Malgieri 2019, 25). The requirements set for human oversight in AIA Art. 14 could, in turn, support the fulfilment of the right to human intervention under the GDPR. AIA Art. 14 requires, among other specific factors, that high-risk AI systems be designed and developed so that natural persons can effectively oversee them. Under AIA Art. 14(4), the humans overseeing the ARSs should understand its capabilities and limitations, monitor the ARS, be aware of automation bias, be able to interpret the output and decide on disregarding, overriding or reversing the input or intervening in the operation where necessary.

[1253] (WP29 2018a, 27; Dreyer and Schulz 2019, 27).

[1254] (WP29 2018a, 27).

[1255] The WP29 has highlighted that there should be 'a simple way for the data subject to exercise these rights', see (WP29 2018a, 27).

[1256] (Wachter and Mittelstadt 2019, 571). As will be discussed in more detail in section 6.1.3.1 below, under the GDPR, procedural complaints related to the processing of personal data in the ADM procedure are possible, such as contesting decisions made based on incorrect or incomplete data. Yet, the normative standards governing the lawfulness of the grounds for the decisions are to be found in other legislation, such as the Non-Discrimination Directives and the national legislation implementing those.

[1257] (Kamarinou et al. 2016, 15).

5.3 Implications of the key legal parameters for employers

The framework of key legal parameters for using ARS demonstrates that ARS deployment triggers numerous legal parameters that vary in their strictness,[1258] normative target,[1259] scope, realisation mechanism, and sanctions for non-compliance.

The bans set the most evident limits and constraints on the ARSs and their use. However, even the bans leave considerable room to manoeuvre for employers, prohibiting only a few specific practices absolutely under all circumstances, such as collecting information on pay history and social scoring of job applicants. Other bans, such as those on direct and indirect discrimination and on processing special category data, have a wider scope, applying to all ARSs but with certain exceptions. Although there is no comprehensive ex-ante oversight of adherence to the bans, the substantial administrative fines for non-compliance serve as a deterrent against banned practices. Nevertheless, despite a commitment to compliance, employers may encounter compliance challenges, particularly with intractable ARSs as will be discussed below.

By virtue of their generality and broader scope, the obligations could have more profound effects, imposing constraints on all kinds of ARS and their use. For instance, the general obligations deriving from the GDPR, such as the principles of processing personal data, may render impermissible ARSs that process personal data beyond what is strictly necessary, or LLM-based recruitment systems whose outputs cannot be shown to meet the accuracy principle. The generality of these obligations could be both an advantage and a risk for employers. On the one hand, obligations appear to allow some degree of flexibility in interpretation, providing opportunities for ARS utilisation. On the other hand, if courts interpret these broad obligations in a manner favouring the protection of job applicants, employers may face considerable administrative sanctions, and potentially also compensation claims[1260].

The specific duties, which appear more concrete than the obligations, could affect employers' processes of operating ARSs, for instance, the manner in which ARS-related risks are assessed and mitigated, ARSs are monitored, staff operating them are trained, and job applicants are informed of their use. However, the DPIA requirement is the only specific duty applicable to all types of ARSs, whereas most other specific duties concern only high-risk AI systems or ADM. To the extent that

[1258] These refer to the strictness or permissiveness of the legal constraints and the level of flexibility the legal parameters contain.

[1259] Normative targets in this context refer to the entity or entities the legal parameter is directed at, i.e., the employer or the ARS itself.

[1260] Regarding the compensation claims see section 6.1 below.

the specific duties apply, they primarily shape the procedural and organisational frameworks surrounding the use of high-risk AI systems rather than fundamentally limit their use.

The job applicant's actionable rights that are based on the GDPR's data subject rights are widely applicable and should be considered before any ARS use. Nevertheless, certain actionable rights are more limited in scope. For example, the right to explanation under the GDPR applies only where the ARS involves ADM within the meaning of Article 22[1261], while the similar right under AIA Article 86 is triggered where a significant decision is taken based on the output from a high-risk AI system. Furthermore, some additional safeguards, such as the right to express one's point of view, apply exclusively to ADM. Although enforcing these rights requires proactive efforts by job applicants, employers must consider these rights throughout the ARS's operational lifecycle. These rights often impose technical requirements on ARS design and functionality, potentially restricting the use of certain types of ARSs, such as non-anonymous ones.

The key legal parameters ultimately prohibit only a limited subset of ARS use cases, allowing the deployment of a wide range of ARSs, provided employers adhere to the legal constraints and implement the procedures outlined in the legislation or instructions for use. Since there is variance regarding the strictness and density of the legal parameters governing different types of ARSs, determining the specific type of ARS in question is a crucial first step in achieving compliance.

Comparing ARS types, high-risk AI systems might at first appear to be the most heavily constrained. However, apart from the absolute bans on certain AI practices, the AIA's legal parameters primarily comprise specific duties for employers deploying high-risk AI recruitment systems, which, as noted above, are primarily procedural and organisational in character rather than significantly constraining the feasibility of ARS use. In contrast, many of the stricter parameters, such as the ban on discrimination and the processing of special category data, apply to all ARSs. The most heavily constrained type of ARSs are high-risk AI systems using ADM, although even these systems remain permitted in certain circumstances.[1262]

In any case, the framework of key legal parameters shows that compliance with one instrument, such as the AIA, alone does not guarantee legal permissibility for

[1261] See GDPR Arts. 15(1)(h) and 22(1) and C-203/22 *Dun & Bradstreet Austria*, para 57.
[1262] (Publication II /Parviainen 2022, 240–45).

ARS use.[1263] To illustrate, a high-risk AI recruitment system that involves ADM might be fully compliant with the AIA, but still make automated decisions without a legitimate basis. Another example is an AI system that infers whether the job applicant may be ill: such a system would not fall within the AIA ban on emotion inference, yet it could constitute processing of data concerning health and be banned by GDPR Article 9. In contrast, some practices may be banned by the GDPR, the AIA and the Non-Discrimination Directives simultaneously, such as certain biometric categorisation or social scoring practices. Hence, it is important that employers analyse the ARS they use against all the applicable legal parameters for that system type.

The framework of key legal parameters could offer guidance in the initial EU-level step of the compliance assessment. However, this assessment must be supplemented by an examination of Member State legislation, which may impose additional constraints. For instance, EU labour legislation constitutes only a small fraction of the legal framework examined here, but there may be more relevant national employment legislation, as well as potentially applicable collective agreements and local labour agreements, that employers must also take into account.

Employers bear the ultimate responsibility for complying with the legal parameters. To this end, they must implement appropriate technical and organisational measures to ensure compliance.[1264] Beyond this, employers must also be prepared to demonstrate that compliance, making documentation and record-keeping crucial.[1265] Yet, ensuring compliance alone is not a viable option. Decisions made during the development phase could have a significant impact on employers' ability to comply with the legal parameters, which underscores the importance of rigorous pre-acquisition due diligence and contractual assurances of compliance from ARS providers.[1266] Given the complexity and opacity of many ARSs, employers are substantially reliant on provider-supplied information, and should

[1263] AIA Recital 63 also clarifies that the fact that ARSs are considered high-risk AI systems, and not prohibited under the AIA, does not mean that they could automatically be deemed lawful under other EU or Member State laws. Cf. (Smuha 2024b, 236). *Nathalie Smuha* has envisioned that the AIA 'does set the tone for AI 'red lines' in the EU, possibly making judges reluctant to assess AI applications' compatibility with data protection law and fundamental rights more generally. Smuha has considered it challenging to claim that high-risk systems are unlawful, unless there is a detailed domestic rule that designates particular systems or practices as unlawful.

[1264] From the perspective of data protection this requirement is also established in GDPR Art. 24.

[1265] GDPR Arts. 5(2) and 24(1).

[1266] Of the effects of the decisions made in the previous stages of the system's lifecycle, see section 3.1 above.

seek to negotiate contractual arrangements that secure access to supplementary information and ongoing support from ARS providers.[1267]

Despite all the parties' commitment to compliance with the key legal parameters, challenges may still arise. First, the ambiguity and open texture of several legal parameters complicate the compliance efforts.[1268] Until the CJEU or EU legislators clarify some of the ambiguities, practitioners could benefit from further guidance from the authorities. Second, technical problems with compliance may also arise. For example, it may be impossible to fully prevent the use of proxies[1269] or the inadvertent processing of special category data in intractable LLM-based ARSs. This highlights the importance of ongoing monitoring of system operations, enabling employers to identify and rectify potential non-compliance swiftly.

Clearly, ensuring compliance with the key legal parameters is not a one-off exercise; rather, it demands continuous attention throughout the ARS's lifecycle. Monitoring of high-risk AI recruitment systems is explicitly required by the AIA, and the GDPR's DPIA duty also necessitates continuous assessments. Compliance with the Non-Discrimination Directives also requires continuous monitoring of ARSs in practice, although this is not explicitly required. Even static ARSs may evolve over time, as updates can introduce new features, and the ARS's use and role in the recruitment process may vary during deployment. These changes could also affect how the ARS is categorised and, by extension, the legal parameters applicable to the ARS. For instance, an ARS that initially did not make automated decisions might later evolve to incorporate ADM if human recruiters cease to meaningfully engage in the CV screening process and instead allow the ARS to select the top applicants. Accordingly, employers cannot content themselves with the initial compliance assessment but must continuously monitor the ARSs.

Furthermore, as the legal landscape continues to evolve, constant monitoring of the legal developments also remains critical.[1270] For instance, CJEU case law has already clarified several aspects of ADM constraints under the GDPR.[1271] The AIA appears even more dynamic than the GDPR, for instance, delegating powers to issue standards that could significantly impact how its provisions are implemented in practice.[1272] Additionally, the Guidelines that the Commission shall develop regarding the practical implementation of the AIA will continue to affect the

1267 See (Gallagher 2024).
1268 See also (Lanamäki et al. 2025).
1269 Of this problem in general, see (Cofone 2018, 1413; Prince and Schwarcz 2020, 1281).
1270 (Lanamäki et al. 2025, 2; Publication I / Viljanen and Parviainen 2022, 8–9).
1271 See cases C-203/22 *Dun & Bradstreet Austria* and C-634/21 *Schufa*.
1272 AIA Art. 40 and see also (Ebers 2021, 19). See, e.g., (European Commission 2025c; 2025d).

interpretations, at least until the CJEU rules on the matters.[1273] Moreover, the horizontal direct effect of fundamental rights is also an evolving doctrine, which employers should take note of. For instance, job applicants' claims based on CFREU Article 47 could affect the burden of proof between the parties, potentially raising employers' risks when they use intractable ARSs.

In conclusion, the framework of key legal parameters reveals that only a few ARS use cases are outright prohibited, and the use of ARSs remains permitted as long as the multiplicity of legal parameters is noted and complied with.[1274] However, it remains to be seen how strictly the CJEU will interpret the legal parameters. Given the CJEU's established teleological approach and record of fundamental-rights-protective interpretations,[1275] stricter readings of, for instance, the principles of processing personal data or the justification possibilities of discriminatory ARSs remain plausible. Such interpretations could render certain intractable ARSs, including LLM-based recruitment systems, impermissible.

Nevertheless, ex-ante oversight mechanisms are basically limited to prior consultation of data protection authorities in the few cases where employers, after a DPIA, report problems in ensuring data protection. Hence, the risk that non-compliance with the legal parameters is noted could remain modest, because enforcement faces several structural problems. When analysing the legal parameters from the job applicants' perspective, the next chapter will also discuss these problems.

1273 See AIA Art. 96.

1274 Yet, a question for another interdisciplinary dissertation could be how to practically build and deploy an ARS that complies with all the legal parameters.

1275 See sections 1.3.1 and 1.4.2 above.

6 Legal Safeguards Against Data Protection Infringements and Discrimination

6.1 Different types of legal safeguards available to job applicants

This chapter addresses the second aim of this dissertation by examining the existing EU-level safeguards for job applicants and evaluating whether they are structurally adequate to protect job applicants against data protection infringements[1276] and discrimination[1277] arising from the use of ARSs. The first subchapter maps the legal safeguards EU legislation provides for this purpose, analysing both their content and adequacy. The second subchapter reviews the identified shortcomings of the safeguards, using LLM-based recruitment systems as a case example. The third subchapter briefly examines interpretive avenues to strengthen the safeguards, even without legislative reform.

Before mapping the safeguards, it is necessary to clarify what is meant by the term. Although legal safeguards are quite often discussed in legal scholarship,[1278] and, for instance, the GDPR requires the implementation of appropriate safeguards in legislation[1279], there does not appear to be a unified definition of legal safeguards. In prior research, two distinct categories of legal safeguards appear to emerge: ex-ante preventive safeguards, which aim to prevent rights infringements, and ex-post

[1276] Data protection infringements are understood broadly as breaches of the GDPR and the CFREU Art. 8.

[1277] Discrimination is also understood broadly, in line with CRFEU Art. 21, to include any form of discrimination, such as direct discrimination, indirect discrimination, and harassment. However, the analysis centres on direct and indirect discrimination. See also CFREU Art. 20 and 23, as well as Art. 2 of the RED, EED and GED.

[1278] See, e.g., (Smuha 2024a, 230–96; Dubal 2025, 403; Enarsson et al. 2022; Suksi 2020, 4; De Hert et al. 2009; Ferrajoli 2001, 7; Abraha 2023, 180; EDPS 2017, 5).

[1279] See, e.g., GDPR Arts. 9(1), 10, 22(2)(b) and 88. The GDPR requires appropriate and suitable safeguards to be implemented by controllers, for example, when making automated decisions (Art. 22(3)).

reactive safeguards, which offer means of redress when infringements occur.[1280] This dissertation adopts that starting point, deeming legal safeguards as the rules and mechanisms established by law to protect job applicants against and in the event of infringement of their rights. However, this dissertation departs from a strictly binary division of safeguards. Hence, in addition to preventive safeguards aimed at deterring rights infringements in advance and remedial safeguards available in case of suspected infringements,[1281] informational safeguards are acknowledged as a separate category.

The analytical justification for this tripartite categorisation of safeguards can be illustrated with reference to the right of access under GDPR Article 15. Under a binary framework, the right would have to be classified as either preventive, because invoking it before a decision is made could prevent inaccurate data from influencing the outcome, or as remedial, because invoking it after a decision could provide evidence for a subsequent claim. Yet, in practice, the right of access functions as both, and classifying it in either category alone would misrepresent its operation and lead to disregarding its full potential and effects. The tripartite categorisation of safeguards resolves this by including the distinct category of informational safeguards, which encompasses measures whose primary function is to shape the flow of information between the parties and can produce both preventive and remedial effects.[1282] This tripartite taxonomy aims to map more precisely what each safeguard type does, and when and how it operates. Nevertheless, the safeguards are not mutually exclusive, and their combined effect must also be considered.[1283]

1280 See, e.g., (Shavell 1993, 257–58; Suksi 2020, 4; Smuha 2024a, 254).

1281 Acknowledging both substantive and procedural protections, see, e.g., (Barnard 2023; Ferrajoli 2001, 23–29). In *Luigi Ferrajoli*'s division, the preventive safeguards are seen as the primary guarantees, that is, the 'duties and prohibitions relative to the rights'. The procedural safeguards, for their part, are secondary guarantees, i.e. duties to apply sanctions if the primary guarantees are not met.

1282 For the rationale behind this categorisation, see also section 1.4.3 above. Another option would have been to include the automatically provided information in the preventive safeguards and the information accessible only when requested as part of remedial safeguards. For instance, in the AIA, the right to explanation has been situated in Chapter IX, 'Post-Market Monitoring, Information Sharing and Market Surveillance', 'Section 4: Remedies'.

1283 For instance, in prior research, it has been suggested that the rights under data protection law should be utilised alongside non-discrimination law; see, e.g., (Aloisi 2024; Parodi 2024; Gaudio 2023; Abraha 2023; Calvi 2023; Grozdanovski 2021; Borgesius 2020). Now, the AIA should also often be included in the analysis.

This subchapter approaches the safeguards from the job applicant's perspective.[1284] Preventive safeguards are evaluated to determine what protections they actually provide to job applicants and how they can enforce the safeguards in case of non-compliance.[1285] Informational safeguards are analysed by asking what information is available to job applicants and whether it suffices to deter infringements and to enable them to seek redress. Finally, remedial safeguards are evaluated by probing whether they can provide an effective means of redress once an infringement has occurred, covering both the accessibility of the procedures and their potential outcomes.[1286]

6.1.1 Preventive safeguards

Preventive safeguards are understood as ex-ante measures aimed at precluding rights infringements.[1287] These safeguards impose constraints on employers that apply regardless of whether any individual applicant invokes them or even knows about them.[1288]

At first sight and on paper, EU legislation appears to include several preventive safeguards that protect job applicants' rights to data protection and non-discrimination. Although some preventive safeguards may be framed as either data protection or non-discrimination measures, many of these could preclude both types

[1284] In terms of *Martti Koskenniemi's* framing of what the law does (Koskenniemi 2025, 20), this subchapter focuses more on what the legislation governing ARS use *empowers* job applicants to do, while Chapter 5 focused more on how the legislation limits and constrains ARSs.

[1285] The discussion of preventive and informational safeguards revisits issues addressed in Chapter 5, but focuses on how the legislation translates into protection for the individual job applicant.

[1286] The key legal parameters focus primarily on preventive or informational safeguards, while offering relatively few remedial measures, such as complaint and sanction mechanisms. This limitation is largely due to the framework's focus on the use phase and its EU-level approach, while remedial matters are largely left to Member States' discretion. As discussed in Chapter 5, the GDPR and the AIA impose penalties for breaches of certain provisions. However, many procedural questions are left to the Member States to decide. See also GDPR Arts. 83–84 and AIA Art. 99. In the Non-Discrimination Directives, all the sanctions are left for the Member States' discretion, as long as those are effective, proportionate and dissuasive. See RED Art. 15, EED Art. 17 and GED Art. 18.

[1287] See, e.g., (Shavell 1993, 257–58; Suksi 2020, 4; Smuha 2024a, 254).

[1288] Broadly, all the key legal parameters introduced in section 5.2 could be considered preventive safeguards. However, some of the legal parameters appear to primarily serve an informational or remedial role and are thus discussed in the following sections. For a more precise discussion of the scope and contents of the preventive safeguards, see section 5.2 above.

of rights infringements. The protection that the preventive safeguards offer depends on the employers' compliance. Since ex-ante external oversight of ARSs is limited, the effectiveness of preventive safeguards could depend heavily on enforcement measures.

From the job applicants' perspective, it is relevant to know what protection the safeguard provides in practice, if the employer complies with it. Furthermore, they should also know how legal protections can be enforced when employers are non-compliant, and what their role is in triggering that enforcement.[1289] The following subsections will address these questions across the four categories of legal parameters that contain mainly preventive safeguards, namely absolute bans, qualified bans, obligations and specific duties.

6.1.1.1 Absolute bans: unconditional prohibitions with limited reach

As regards the protection they provide, the strictest preventive safeguards are the absolute bans that unconditionally restrict certain ARS uses.[1290] In the recruitment context, the bans are non-waivable, which strengthens their force.[1291] However, the scope of these absolute bans is very narrow, applying primarily to specific practices in AI systems[1292] which the legislature has considered particularly harmful and abusive.[1293] Yet many problematic ARS uses fall entirely outside the scope of the absolute bans.

Only four of the AIA's absolute bans appear relevant in the recruitment context, and even these bans have a somewhat limited scope. The most significant of these bans is arguably the ban on social scoring. Scores derived from unrelated contexts could, for example, be used to screen job applicants, leading to detrimental treatment based on data that is neither accurate nor necessary for recruitment, raising clear data protection concerns. Because ostensibly neutral data may also serve as proxies for protected characteristics, such scores may lead to discriminatory outcomes, making this ban relevant to equality as well.[1294] The ban on biometric categorisation systems

1289 The remedial procedures will be discussed in more detail in section 6.1.3, and the general difficulties with enforcement will be discussed further in section 6.2.

1290 See section 5.2.1.1 above.

1291 For instance, *Karen Yeung* has considered the waivability as one of the main shortcomings of the human rights framework in the digital age (Yeung 2018, 70–71).

1292 In addition to the AIA, the PTD also contains an absolute prohibition of asking for pay history applicable in all types of recruitment processes.

1293 See AIA Art. 5 and Recital 28.

1294 AIA Art. 5(1)(c) and (European Commission 2025c, 50). However, similar preventive effects could also stem from the GDPR's principles of processing personal data and the prohibition of ADM. Non-Discrimination Directives could also prevent social scoring practices, if those amount to direct or indirect discrimination.

explicitly prohibits certain processing of special category personal data, thereby restricting certain targeted job-advertisement practices that could otherwise lead to both data protection violations and discrimination.[1295] The bans on decision manipulation and exploitation of vulnerabilities could prevent some significantly harmful practices, but are unlikely to apply in the recruitment context.[1296]

Beyond the AIA, the PTD's specific ban on using pay history introduces an additional preventive safeguard, as it excludes a data point that reflects past inequalities and is often unnecessary for assessing a candidate's suitability for a position.[1297] Yet, the PTD's enforcement framework and the precise scope of this ban are determined primarily at the Member State level, and the degree of protection it affords may therefore vary across jurisdictions.[1298]

Given the close links between absolute bans, non-discrimination, and data protection, many of the practices that are absolutely banned are also constrained by other legislation. However, the explicit articulation of these bans, particularly in the AIA, could enhance their enforceability. For instance, in cases involving prohibited social scoring, job applicants could claim a breach of the AIA's ban rather than relying on the GDPR's principles for processing personal data and the provisions of national non-discrimination legislation.

Nevertheless, the enforcement possibilities under the AIA are constrained, as it does not provide a right to judicial remedies or compensation for job applicants in the event of infringement.[1299] Hence, job applicants must rely on national legislation to bring claims for breaches of the AIA, unless the breach simultaneously infringes the GDPR. In cases based solely on the AIA, the extent of recoverable damages and the possibility of bringing a claim will ultimately depend on national legislation.[1300] Private enforcement,[1301] especially in courts, faces a universal challenge of detecting infringements and obtaining the necessary evidence to prove them.[1302] While the informational safeguards could provide some assistance in this regard, they are by no means a panacea.[1303]

1295 AIA Art. 5(1)(g).
1296 See section 5.2.1.1 above and AIA Art. 5(1)(a) and 5(1)(b).
1297 See PTD Art. 5(2).
1298 See section 5.2.1.1 above.
1299 See also (Publication IV / Parviainen 2026).
1300 National non-discrimination legislation may provide an avenue for obtaining compensation if, for instance, the social scoring amounts to discrimination. Otherwise, job applicants would have to resort to national tort law.
1301 Of private enforcement, see, e.g., (Shavell 1993, 267–68; Lafarre 2023, 233–35).
1302 See, e.g., (Gerards and Xenidis 2020, 69, 74; Kelly-Lyth 2023, 167–68). See also section 6.2 below.
1303 See section 6.1.2 below.

Nonetheless, job applicants' complaints to market surveillance authorities are enabled in the AIA.[1304] The authorities' investigations could reveal infringements and provide evidence of those.[1305] Furthermore, those may lead to significant administrative fines and other consequences for the employers.[1306] Considering the job applicants' lack of judicial remedies under the AIA, the preventive effect of the absolute bans depends significantly on the credibility of public enforcement and the ensuing sanctions.[1307]

6.1.1.2 Qualified bans: broad coverage with undermining exceptions

As regards the protection they provide, many *qualified bans* have a broader material scope than absolute bans and could thus establish more widely applicable preventive safeguards. Many of the qualified bans must be noted in all algorithmic recruitment situations. Similar to the absolute bans, the AIA's and the GDPR's qualified bans protect both data protection and non-discrimination rights,[1308] while the bans on discrimination focus on preventing discrimination.[1309]

In all algorithmic recruitment, the prohibitions against direct and indirect discrimination[1310], and against processing special category personal data[1311] or personal data related to criminal convictions,[1312] protect job applicants. However, under EU secondary law, their applicability is restricted to an exhaustive list of protected grounds[1313] or types of personal data.[1314] The applicability of the bans on discrimination could be broadened by the CFREU Article 21, which prohibits all kinds of discrimination and provides a non-exhaustive, broader list of protected grounds.[1315] Yet, the CFREU applies only when the situation falls within the scope

1304 AIA Art. 85.
1305 See also (Publication IV / Parviainen 2026).
1306 See AIA Art. 99 and Art. 14 of the Market Surveillance Regulation.
1307 See also (Shavell 1993, 261–62).
1308 For instance, AIA Art. 5(1)(f) ban on inferring emotions in the workplace tackles the unreliability of such systems (see, e.g., (Barrett et al. 2019; European Commission 2025c, 81)) and their potential to process inaccurate data, especially for underrepresented groups, which might lead to discriminatory outcomes. See also AIA Recital 44. Of the well-known problems of facial recognition systems in detecting darker faces, see e.g., (Buolamwini and Gebru 2018).
1309 See also GDPR Recital 71.
1310 RED Art. 2, EED Art. 2 and Art. 14 of the GED.
1311 GDPR Art. 9.
1312 GDPR Art. 10.
1313 RED Art. 1, EED Art.1 and GED Art. 1. See also section 5.2.1.2 above.
1314 GDPR Arts. 9 and 10. See also section 5.2.1.2 above.
1315 In some situations, also CFREU Art. 20 or 23 could come into question. See also (Publication III / Parviainen 2024, 452–53).

of EU law,[1316] and invoking it could require more knowledge from job applicants than invoking the secondary law directly. Although these qualified bans initially seem widely applicable, certain characteristics of ARSs, such as their complexity, intractability, and use of proxies, could limit the practical applicability of, especially, the qualified ban on direct discrimination.[1317]

Furthermore, some qualified bans have a much more limited scope.[1318] The ban on ADM targets only solely automated decision-making,[1319] which does not take place in all algorithmic recruitment processes.[1320] However, because the scope of the ban on ADM remains unspecified in the recruitment context,[1321] courts may ultimately find more ADM than currently anticipated, providing broader protection to job applicants. In any case, the ban on ADM is not dependent on any specific technologies or detailed types of personal data. In contrast, the AIA's two qualified bans on inferring emotions in the workplace[1322] and on criminal risk assessment[1323] apply only to specific practices in AI systems.

The protection that qualified bans offer to job applicants, however, is curbed by their inherent exceptions. As exceptions to rules that protect fundamental rights, all these exceptions should be interpreted restrictively.[1324] Yet, the likelihood that the exceptions apply varies between the bans. The exceptions under the AIA's qualified bans and direct discrimination could be the least likely to apply, while the broad justification possibilities of the indirect discrimination ban could make it the most likely to be exceptionally justified. The GDPR's bans are likely to lie somewhere between these two extremes.

1316 CFREU Art. 51(1). See also Case C-617/10 *Åkerberg Fransson*, paras 19-23 and 28; and C-206/13, *Siragusa*, paras 25-30. See also (Publication III / Parviainen 2024, 454), where I suggested that the CFREU could apply when the GDPR or the AIA are applicable to the ARS.

1317 (Williams et al. 2018; Cofone 2018; Gerards and Xenidis 2020, 44). In Publication III, I proposed that there could still be situations in which the prohibition of direct discrimination could also apply (Publication III / Parviainen 2024, 463–64) and section 4.3 above.

1318 The qualified bans on special category personal data processing and automated decision-making might, in very exceptional situations, be waivable by job applicants' consent, see (Publication II /Parviainen 2022, 245).

1319 GDPR Art. 22. See also sections 2.3, 4.2 and 5.2.1.2 above.

1320 (ICO 2024, 32; Carter 2024, 351–52).

1321 See sections 5.2.1.2 and 4.2 above.

1322 AIA Art. 5(1)(f).

1323 AIA Art. 5(1)(d).

1324 In the context of privacy and protection of personal data, see, e.g., cases C-73/07 *Satakunnan Markkinapörssi*, para 56, C-293/12 *Digital Rights Ireland,* para 52 and C-473/12 *IPI*, para 39.

Turning first to the AIA's qualified bans, the ban on inferring emotions at the workplace appears particularly strong in the recruitment context, as safety and medical reasons capable of justifying its use are unlikely to exist there.[1325] Similarly, the exceptions to the AIA's ban on criminal profiling are relatively unlikely to apply if Member State legislation does not allow the employer to process personal data related to criminal convictions.[1326]

Moving on to non-discrimination, the ban on direct discrimination appears to be a relatively robust safeguard on paper, as less favourable treatment based on the protected grounds may be justified only exceptionally where explicitly permitted under Member State legislation.[1327] Hence, if direct discrimination can be established in court, employers are unlikely to find a justification for the less favourable treatment of job applicants.[1328] However, as discussed above in section 5.2.1.2, and particularly in Publication III, the ban on direct discrimination may be less well-suited to addressing discrimination in ARSs than its indirect counterpart.

Although more ARSs could fall within the scope of the prohibition of indirect discrimination, which could also better cover proxy discrimination,[1329] its preventive effect is notably diluted by the justification clause included in the Directives.[1330] Namely, indirect discrimination is not deemed to take place, even when an apparently neutral provision, criterion or practice puts persons at a particular disadvantage compared to other persons, if the 'provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary'.[1331] Prior scholarship, drawing on CJEU case law,

1325 AIA Art. 5(1)(f) and section 5.2.1.2 above.

1326 AIA Art. 5(1)(d) and section 5.2.1.2 above. See also GDPR Art. 10, which restricts the processing of personal data related to criminal convictions.

1327 See section 5.2.1.2 above. See, e.g., RED Art. 4, EED Art. 4 and GED Art. 14(2). The EED leaves room for more national exceptions on grounds of age (Art. 6) and for generally protecting the rights and freedoms of others (Art. 2(5)). For the limits of direct discrimination, especially from the perspective of substantive equality, see, e.g., (Fredman 2022, 279–80).

1328 (Publication III / Parviainen 2024).

1329 (Gerards and Xenidis 2020, 67, 70–71; Hacker 2018, 1153; Xenidis and Senden 2020, 172; Martínez-Ramil 2022; Wachter et al. 2021, 20; Carter 2024, 358; Rigotti and Fosch-Villaronga 2024, 5).

1330 If the ARS is evaluated to be discriminatory based on the CFREU Art. 21, the justification possibilities appear rather similar to those under the indirect discrimination cases. Namely, based on the CJEU case law, different treatment may be objectively justified if its aim is legally permitted and the treatment is proportionate to the aim pursued. See cases C-356/12 *Glatzel*, para 43 and C-406/15 *Milkova*, para 55. See also (Publication III / Parviainen 2024, 452).

1331 See RED Art. 2(2)(b), EED Art. 2(2)(b) and GED Art. 2(1)(b). See also C-170/84 *Bilka-Kaufhaus*, para 36, C-157/15 *Achbita,* paras 35 and 43, C-144/04 *Mangold,* para 65. For a more detailed discussion, see section 5.2.1.2 above.

suggests that the justifications could be applicable relatively often in algorithmic discrimination, including in the recruitment context.[1332] This interpretation seems to be based on the assumptions that: (i) in the algorithmic recruitment context several legitimate aims (e.g. evaluating future job performance) could exist;[1333] (ii) algorithmic systems could be an appropriate means to achieve those aims, due to their predictive capacities, among other factors;[1334] and (iii) other less discriminatory means would not exist (e.g. as human recruiters tend to discriminate as well).[1335] Nevertheless, as the CJEU has not yet decided on the justifiability of algorithmic systems that lead to placing persons at a particular disadvantage, a stricter interpretation of the justification possibilities in an algorithmic recruitment context appears still possible.[1336]

Turning to the qualified bans in the GDPR, the exceptions to processing special category personal data and criminal conviction data, as well as conducting ADM, may sometimes apply in the recruitment context. Yet, at the moment, there is no one categorical exception that would always apply in algorithmic recruitment,[1337] and each case must be analysed separately. For instance, there may be national employment legislation that demands the processing of special category personal data[1338] or data on criminal convictions.[1339] Furthermore, ADM could be permitted in recruitment if it is necessary for entering into an employment contract due to an extremely high number of applications, and in very few cases, based on the job applicant's explicit consent, if it is deemed exceptionally valid.[1340]

Given these exceptions, the qualified bans offer broader initial coverage than the absolute bans but less certainty. Initially, employers assess whether the exceptions apply. In the rare cases where the employer consults a data protection authority after a DPIA, the authority may take a stance on the applicability of GDPR Article 9 or 22 exceptions, but not necessarily on the exceptions related to the AIA or Non-

1332 See section 5.2.1.2 above. Of the justification possibilities, especially in the recruitment context, see, e.g., (Martínez-Ramil 2022). From the UK perspective, see also (Kelly-Lyth 2021, 906–7).

1333 (Hacker 2018, 1161; Martínez-Ramil 2022, 14).

1334 (Hacker 2018, 1162).

1335 (Hacker 2018, 1162; Martínez-Ramil 2022, 13).

1336 Of such possible interpretations, see section 5.2.1.2 above and 6.3 below.

1337 Cf. If processing of special category personal data is deemed necessary to comply with the Non-Discrimination Directives, as some scholars have suggested (Žliobaitė and Custers 2016), the exception under GDPR Art. 9(2)(b) could apply widely.

1338 National legislation may, for instance, demand the processing of vaccination data in certain instances. See (Publication I / Viljanen and Parviainen 2022, 3).

1339 For a Finnish example, see section 5.2.1.2 above and Sections 2 and 3 of the Act on checking the criminal background of persons working with children.

1340 GDPR Art. 22(2). See also (Publication II /Parviainen 2022, 240–45). For a more detailed discussion of these, see also section 5.2.1.2 above.

Discrimination Directives' prohibitions.[1341] In the vast majority of cases, the protection the qualified bans offer depends on how employers and, ultimately, courts interpret the exceptions in relation to specific ARSs. The discretion left to the employers risks making the protection contingent rather than assured. Particularly, as assessing the applicability of the exceptions is not a simple task, which may often[1342] involve balancing competing interests (e.g., job applicants and employers).[1343] Hence, ex-post enforcement appears to be crucial for ensuring compliance with qualified bans.

As regards enforcement of non-compliance, public enforcement by supervisory authorities is possible during deployment: the authorities may inspect the ARSs either on their own initiative or in response to a job applicant's complaint.[1344] Additionally, job applicants could raise a claim directly in court when they consider the qualified bans to be infringed, but this requires considerable resources and faces several challenges, including detecting breaches and proving them.[1345] Furthermore, as will be discussed in more detail below in section 6.1.3, only the GDPR provides a judicial remedy directly; for breaches of the AIA and the Non-Discrimination Directives, job applicants must rely on national legislation and potentially CFREU Article 47. Compared to the absolute bans, the existence of the exceptions raises the risk of unsuccessful claims, as an ARS that initially appears banned may be exceptionally justified.

Nevertheless, the enforceability of the qualified bans also varies. For example, a breach of the ban on processing special category personal (GDPR Article 9) might be detected from the information obtained via a data access request made under GDPR Article 15. While this might also reveal indicia of discrimination, the breach of the GDPR Article 9 might be simpler to prove, as the job applicant would not have

1341 However, if the same authority acts as the data protection and market surveillance authority, they might also proactively check AIA compliance in these situations.

1342 This is the case, for instance, when considering the necessity of ADM for entering into an employment contract or the justifiability of a certain disadvantaging ARS.

1343 The employer's freedom to conduct business is also recognised in the CFREU Art. 16. See also case C-426/11, *Alemo-Herron*. Nevertheless, also other pairs for comparison could emerge, such as job applicants' right to data protection and ARS providers' trade secrets, which might emerge when analysing the scope of job applicants' right of access under GDPR Art. 15. Furthermore, environmental protection interests (CFREU Art. 37) should also increasingly appear in the balancing exercises, considering the huge environmental impacts that the AI systems have. See also (Hacker 2024b). Environmental interests could typically weigh against ARS use and hence support job applicants' cases. Nevertheless, if the ARSs were to provide the benefits envisioned, e.g., regarding less biased decision-making, the environmental interests could conflict with the interests of both job applicants and the employer.

1344 See AIA Art. 85 and GDPR Art. 77.

1345 See section 6.2 below.

to show that the infringement has caused any detrimental effects on them.[1346] The breach of the ban on special category data could lead to significant administrative fines[1347] and other detrimental consequences for the employer,[1348] and the threat of these could have a preventive effect. However, to receive compensation, job applicants must also demonstrate the damage and its connection to the breach.[1349] In contrast, contesting employers' use of ADM could be particularly tricky, as the job applicants could struggle to show that the human involvement has not been meaningful.

Moreover, in discrimination cases, job applicants have exceptionally[1350] an alleviated burden of proof, meaning that establishing a prima facie case of discrimination requires only establishing facts on the basis of which it may be presumed that discrimination has taken place.[1351] However, the burden of proof is not reversed, meaning that job applicants must still sufficiently demonstrate the particular harm, the protected group in which it takes place and its disproportionality compared to others in a similar situation.[1352] If the burden of proof is interpreted to shift to employers at a lower evidentiary threshold in cases where the ARS is opaque, and job applicants' ability to establish facts is limited, the bans on discrimination could have broader preventive effects, especially if the sanctions are sufficiently high.[1353] However, sanctions in discrimination cases may differ considerably between Member States.[1354]

Overall, the job applicants' possibilities to enforce qualified bans may be somewhat higher than enforcing the absolute bans, where EU legislation does not

1346 *Steven Shavell* has analysed different law enforcement dimensions, including stages of intervention. He has divided the stages of intervention into prevention, act-based sanctions and harm-based sanctions. See (Shavell 1993, 257–58). The GDPR and the Non-Discrimination Directives diverge along these lines. The Non-Discrimination Directives provide mainly harm-based sanctions, whereas the GDPR provides both harm-based and act-based sanctions. The right to compensation under GDPR is harm-based, whereas the administrative fines and other supervisory authorities' measures are act-based.

1347 GDPR Art. 83.

1348 The data protection authorities have, for instance, the powers to issue warnings, reprimands, orders to comply and ban certain processing. See GDPR Art. 58.

1349 See, e.g., cases C-300/21 *Österreichische Post*, para 42 and C-456/22 *Gemeinde Ummendorf*, paras 22–23.

1350 Similar alleviations are not explicitly awarded in the data protection or AIA infringement cases, at least not based on EU legislation. For a more detailed discussion on this, see section 6.1.3.2 below.

1351 EED Art. 10, RED Art. 8 and GED Art. 19. See also (Publication III / Parviainen 2024).

1352 (Wachter et al. 2021, 7–14).

1353 Of the level of sanctions needed for harm-based sanctions, such as those of the Non-Discrimination Directives, to have deterring effects, see, e.g., (Shavell 1993, 261–62).

1354 (Chopin and Germaine 2023, 102–6).

directly provide for judicial remedies or alleviated burden of proof. Nevertheless, the combination of exceptions, detection difficulties, and evidentiary requirements means that enforcement of qualified bans in individual cases still remains demanding for job applicants.

6.1.1.3 Obligations: generally applicable yet vague

Several legal parameters that are categorised as *obligations* in Chapter 5 also constitute preventive safeguards. Especially the GDPR-based obligations have a broad scope, and their preventive effects should extend to most ARSs. For instance, the obligations to ensure a lawful ground for processing personal data[1355], to follow the principles of processing personal data[1356], and to ensure compliance with data subject rights and transparency[1357] must be noted in all ARS. The EED-based obligation to provide reasonable accommodations applies also to all ARSs.[1358] However, there are a few obligations applicable only to (high-risk)[1359] AI systems[1360] and systems conducting ADM.[1361]

The GDPR's general obligations applicable to all ARSs are foundational.[1362] For instance, if personal data is processed unlawfully from the outset, such as without a legal basis for processing, no subsequent technological or organisational measure, nor any amount of human oversight, monitoring, logging, informing or reporting can fully remedy the initial breach. The obligation to have a lawful ground for processing personal data could prevent the use of possibly harmful ARS features, such as systems that conduct in-depth analysis of applicants' social media profiles.

Furthermore, the GDPR's obligations could often help prevent both data protection infringements and discrimination. For instance, the principles of data minimisation[1363] and accuracy[1364] could help safeguard against discriminatory outcomes and data protection infringements by reducing reliance on unnecessary or inaccurate data. However, the ARSs' characteristics, such as their ability to process vast amounts of personal data and LLM-based recruitment systems' tendency to confabulate, could pose challenges to the application of these principles. Yet, the

1355 GDPR Art. 6.
1356 GDPR Art. 5.
1357 GDPR Arts. 12-14.
1358 EED Art. 5.
1359 AIA Art. 48–49 and 71.
1360 AIA Art. 50.
1361 GDPR Art. 22(3).
1362 See, e.g., (EDPB 2024b, 19–21).
1363 GDPR Art. 5(1)(c).
1364 GDPR Art. 5(1)(d).

principles may be interpreted in a manner that protects fundamental rights and ensures their preventive effects, as will be discussed below in section 6.3.[1365]

In contrast, the EED's requirement of reasonable accommodations aims to safeguard, especially, the equal treatment of job applicants with disabilities and has a more limited personal scope.[1366] Although seemingly targeted only to combat disability discrimination, such measures may nevertheless promote the accuracy of data processing more broadly. For instance, if reasonable accommodations are anticipated by including accessibility features in ARSs, those features (e.g., screen readers, text resizing, or plain language options) could help all applicants provide relevant and accurate personal data.

While the scope of the AIA's obligations is rather limited, those are more specific than the GDPR-based obligations, making them potentially easier to comply with and to enforce.[1367] In comparison, the GDPR's obligation to have suitable safeguard measures in place when ADM is used leaves considerable discretion to the employer.[1368]

Vagueness is a common feature of the obligations.[1369] While it could offer flexibility and enable the obligations' preventive effects to encompass future ARSs, it also gives employers considerable power regarding the implementation of the preventive safeguards. Furthermore, given the lack of case law and limited guidance from supervisory authorities on implementing these obligations in the algorithmic recruitment context, employers may struggle to comply with them in practice.[1370] Accordingly, the vagueness of the obligations may diminish their preventive effects and the level of protection they offer to job applicants.

Moreover, the vagueness of the obligations also complicates enforcement. Similarly to employers, job applicants struggle to determine what the obligations actually require and whether they have been breached, which could prevent them from initiating enforcement. Further, the vagueness increases uncertainties in enforcement procedures and diminishes legal certainty, as it can be challenging to anticipate how courts will interpret the obligations in individual cases. Taken

1365 See also section 5.2.2 above.
1366 EED Art. 5. Of the possibility to deem systems that lack accessibility functions as indirectly discriminatory, see (Kelly-Lyth 2023, 166; Daly and Whelan 2021, 750).
1367 See AIA Arts. 48–50 and section 5.2.2 above.
1368 See GDPR Art. 22(3) and section 5.2.2 above.
1369 See, e.g., GDPR Art. 5. While Recital 39 provides some specification, further clarification is expected to develop through case law and supervisory authority guidance.
1370 See also section 5.2.2 above and 6.2 below.

together, these factors could diminish the willingness of job applicants to bring claims against employers in court, which the GDPR would allow.[1371]

Accordingly, complaints to supervisory authorities may be the most likely enforcement avenue, potentially leading to significant administrative sanctions and measures in cases where breaches of the GDPR's obligations are found.[1372] In theory, compliance with the GDPR's obligations can also be evaluated ex ante by data protection authorities if they are consulted prior to ARSs adoption, as will be discussed in the next section. If the job applicants choose to bring claims directly in court, they must overcome the difficulty of demonstrating that the obligation was breached. The vagueness of the obligations might perpetuate the informational asymmetries between the job applicants and employers here. Employers can point to a range of measures taken as evidence of compliance with the obligations, while job applicants have a hard time specifying what employers should have done differently. This asymmetry is likely to make the supervisory authority complaints the more realistic primary enforcement route, as it may also provide job applicants with some of the information required for judicial claims.[1373]

6.1.1.4 Specific duties: DPIA leading to potential ex-ante oversight and various preventive measures for high-risk AI systems

The specific duties that EU legislation imposes on employers also include important preventive safeguards. Compared to the general obligations, the specific duties are more targeted in two respects. First, unlike the obligations, many of the specific duties apply only to high-risk AI systems, thereby limiting the scope of their protection.[1374] However, the duty to conduct a DPIA may apply to all types of ARSs that process personal data, regardless of the type of technology used.[1375] Second, the specific duties set out more clearly defined requirements for employers, which could make compliance easier. Yet, as the details of many duties are tied to the providers' instructions for use, the content of those instructions may therefore influence the level of protection that the specific duties afford. Furthermore, as the specific duties are more concrete, it may be easier to evaluate whether they have been breached than in the case of more broadly formulated obligations.

1371 For a more detailed discussion on the claims, see section 6.1.3.2 below. The claims also suffer from the other problems discussed, especially in section 6.2 below.

1372 GDPR Arts. 83 and 58. National legislation determines the sanctions for breaches of the right to reasonable accommodation.

1373 See section 6.1.3 below. Yet, the potentially short time frames for filing suits could limit the usefulness of the claims.

1374 AIA Art. 26. See also AIA Art. 4 on AI literacy that applies to all AI systems.

1375 GDPR Art. 35. See section 5.2.3 above on the scope of the DPIA obligation.

Importantly, apart from supervisory authorities' incidental investigations, the DPIA is currently the only preventive measure through which ex-ante external oversight could potentially be triggered.[1376] Nevertheless, data protection authorities must be consulted only if the employer concludes that it cannot sufficiently address the identified risks.[1377] The consultation duty might be triggered, for instance, in the case of using LLM-based recruitment systems. Due to confabulations, such systems may entail a risk that job applicants are unfairly excluded and irreversibly lose a job opportunity, even after the employer has implemented available safeguards.[1378] However, as this provision also relies on the employers' self-assessment of the residual risk levels, the situations in which prior consultation is sought are likely to be limited.[1379] When the data protection authorities are consulted, they have an opportunity to assess the system's compliance with the GDPR before deployment. Considering, for example, the problems with LLM-based recruitment systems' compliance with the principles of processing personal data,[1380] data protection authorities might ultimately restrict their use.

Even if the DPIA does not require consulting the supervisory authority, it should be a process that identifies risks to multiple fundamental rights and proposes solutions to address these risks.[1381] For instance, excessive data use and discriminatory outcomes could be addressed in the DPIA. However, job applicants' ability to ensure that DPIAs are properly conducted is limited, as they lack access to the documents unless the employer voluntarily makes them public, as encouraged by the WP29.[1382] Yet under GDPR Article 36(3)(e), the employer must disclose the

1376 GDPR Art. 36.

1377 GDPR Art. 36(1), see also Recitals 84 and 94. There do not appear to be any EU-wide statistics on the number of prior consultations. Some data protection authorities have published the numbers of all prior consultations, not only those related to employment. For instance, the Swedish data protection authority reports having received only 12 prior consultation requests in 2024 (Integritetsskydds myndigheten (IMY) 2025, 38).

1378 The WP29 guidelines on DPIAs mention the following as an example of a situation where an unacceptable high residual risk exists: data subject encounters significant, or even irreversible, consequences which they may not overcome, such as a layoff and/or when such a risk will obviously occur (WP29 2017a, 18–19). However, some process-related solutions could be developed to eliminate the risks posed by confabulations; see section 5.2.2 above.

1379 See also (Abraha 2023, 183).

1380 See section 5.2.2 above.

1381 GDPR Art. 35 and Recital 75. See also (WP29 2017a, 16).

1382 The WP29 has encouraged controllers to consider publishing at least some parts of the DPIA (WP29 2017a, 18; 2018c, 22). See also (Kelly-Lyth 2021, 925–27). Furthermore, GDPR Art. 35(9) requires stakeholder involvement in DPIAs, which could allow some employee representatives to access the DPIAs. However, that information might not reach the job applicants.

DPIA documentation to the supervisory authority.[1383] Hence, public enforcement by data protection authorities is crucial to ensure that DPIAs function as a preventive safeguard.

Regarding high-risk AI systems, the AIA's duties imposed on deployers establish several preventive safeguards that may deter both data protection infringements and discrimination. For example, assigning a competent person to oversee the ARSs,[1384] together with the AI literacy requirement, could help prevent or minimise the AI recruitment system's risks to job applicants.[1385] However, another question is how well-equipped humans are to truly prevent the infringements ARSs might cause.[1386] Furthermore, the technical and organisational measures to ensure compliance with the instructions for use[1387], the duty to utilise relevant and sufficiently representative input data[1388] and monitoring of the ARS's operations[1389] should prevent both data protection infringements and discrimination of job applicants when high-risk AI systems are used. Yet, these duties might not add much to the protection provided by the GDPR and the Non-Discrimination Directives, except for making the requirements more explicit.[1390]

Nevertheless, articulating the employers' obligations more explicitly in the AIA could reinforce and extend the preventive effects of the GDPR and Non-Discrimination Directives as well. For instance, introducing an explicit monitoring obligation could help prevent discrimination, as such monitoring is not explicitly mandated in the Non-Discrimination Directives and may therefore be overlooked by employers who are not well-versed in non-discrimination law. Systematic monitoring could enable early detection and prevention of discriminatory outcomes that might otherwise remain unnoticed. Moreover, reporting identified incidents to market surveillance authorities could help ensure that similar risks are addressed collectively, thereby preventing their recurrence or dissemination among other users of the same ARS.[1391]

The specific duties require employers to follow certain procedures, but apart from the information duties under AIA Articles 26(7) and 26(11), they do not offer job applicants any rights to verify that the procedures were followed or to access the

1383 See also (WP29 2017a, 18).
1384 AIA Arts. 26(2) and 14.
1385 See AIA Arts. 4 and 14(2), and Recital 20.
1386 Of the problems of this safeguard, see also section 6.2 below.
1387 AIA Arts. 26(1) and 13(1).
1388 AIA Art. 26(4).
1389 AIA Art. 26(5).
1390 For instance, the duty regarding relevant and representative input data does not necessarily add much compared to qualified bans of the Non-Discrimination Directives and the obligations under the GDPR. See also section 5.2.3 above.
1391 AIA Art. 26(5).

documents that they produce. Hence, similarly to the other preventive safeguards, the protection the specific duties provide depends strongly on employers' implementation measures. Although the greater concreteness of specific duties could assist enforcement efforts compared to the more vague obligations, the fact that most specific duties stem from the AIA limits job applicants' enforcement options.

Namely, the only enforcement option under the AIA is to lodge a complaint with market surveillance authorities.[1392] Nevertheless, the market surveillance authorities' access to information about potential breaches is strengthened by employers' monitoring and reporting duties and providers' obligations, which facilitate enforcement.[1393] Accordingly, these authorities are best placed to ensure compliance with the AIA's specific duties.[1394] However, administrative fines could be issued only for breaches of the deployers' obligations under AIA Article 26 and not separately for the AI literacy obligation.[1395] Breaches of the AIA's duties could be claimed in court, either in relation to breaches of the GDPR and non-discrimination legislation, or separately based on national legislation.[1396] Nevertheless, given the job applicants' limited access to the processes specific duties trigger, they are likely to require supervisory authorities to investigate the ARSs on their behalf prior to bringing claims in court.

The mere existence of job applicants' actionable rights, such as their rights to explanation and access, could also have a preventive effect by increasing the likelihood that potential breaches are detected. However, due to their importance in facilitating the use of remedial safeguards, these will be discussed separately next as informational safeguards.

6.1.2 Informational safeguards

Informational safeguards include legal parameters that should ensure the flow of information from employers to job applicants and may enhance job applicants' understanding of the ARSs. Informational safeguards have both preventive and remedial effects.

First, the transparency requirements, combined with the risk of enforcement actions, could have a preventive effect, incentivising employers to take preventive

1392 AIA Art. 85. See also (Publication IV / Parviainen 2026).
1393 AIA Art. 26(5). See also (Publication IV / Parviainen 2026), where the provider's duties to draw up documentation based on the AIA are also discussed.
1394 See also (Publication IV / Parviainen 2026).
1395 AIA Arts. 99 and 74 and Market Surveillance Regulation Art. 14. For considering neglect of the AI literacy obligation in connection with other breaches, see (Publication IV / Parviainen 2026).
1396 See also section 6.1.3 below.

safeguards seriously. However, the preventive effects of the informational safeguards could be limited if the safeguards are not utilised. Hence, job applicants' or their representatives' active measures and critical engagement are crucial for the effectiveness of the informational safeguards, even if the information would be automatically provided to them.[1397]

Second, the informational safeguards facilitate the use of remedial safeguards. Namely, the informational safeguards should ensure that job applicants are aware of ARS use.[1398] Furthermore, these safeguards may help identify data protection infringements or discrimination. Thus, the informational safeguards could enable job applicants to seek enforcement and redress, potentially also assisting them in gathering evidence for claims against employers.

This section will first discuss the information provided to job applicants upfront, and thereafter, the focus shifts to information that is provided only in response to job applicants' requests.

6.1.2.1 Information provided upfront

Several informational safeguards apply automatically. Basic information regarding personal data processing must be provided, regardless of the type of ARS used, while more specific disclosures may be required only where ARSs involve high-risk AI or ADM.

The GDPR's general transparency obligations established in Articles 12–14 are important as they apply regardless of the type of ARS. Yet, GDPR Articles 13 and 14 do not explicitly require the disclosure of AI use, although complying with the transparency principle could be interpreted as requiring such information, as discussed in section 5.2.2.[1399] The basic information on the processing of personal data[1400] may, nevertheless, occasionally reveal data protection infringements, such as clearly unsuitable lawful bases or unacceptable purposes for processing. However,

[1397] In light of the literature on digital consent and privacy fatigue, most job applicants probably do not even read the privacy notices provided. See, e.g., (McDonald and Cranor 2008; Solove 2013, 1888). Trade unions may act upon information provided to their members, while NGOs may provide support to job applicants outside of union membership.

[1398] However, as has been discussed above in section 5.2.2 and more below in section 6.1.2.1, the information provided could be limited, especially in cases where ARSs do not involve ADM or high-risk AI decision-support.

[1399] See GDPR Art. 5(1)(a) and (WP29 2018a, 25).

[1400] See GDPR Arts. 13(1)–(2) and 14(1)–(2). The information to be provided includes, among other aspects, the purposes of the processing and its legal basis, the legitimate interests if those are used as a basis for processing and the potential recipients or categories of recipients of the personal data and the storage periods.

that information is unlikely to assist in revealing discrimination or major problems in data protection, or in proving such in court.[1401] The fact that GDPR Articles 13(2) and 14(2) require employers to inform job applicants of their data protection rights is important for job applicants' enforcement possibilities, as many average job applicants may not be aware of these rights.[1402]

The AIA Article 50 obligations, which demand transparency of AI systems that directly interact with job applicants and the marking of artificially generated content, could also increase job applicants' awareness of the AI systems used.[1403] However, these disclosures are unlikely to furnish information that could assist in enforcement actions.

Potentially more valuable informational safeguard is included in GDPR Articles 13(2)(f) and 14(2)(g), which require further information to be provided, at least in the case of ADM. The wording 'at least' suggests that further information could also be provided if there is no ADM, and the WP29 has also suggested that as a good practice.[1404] Before ADM is used, job applicants should be informed of the existence of automated decision-making, including profiling, and given meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[1405] This should ensure that job applicants are aware of when automated decisions concerning them are made and how these decisions may affect them. Since the information should include intelligible details about the procedure and principles used in the automated processing,[1406] it may, in exceptional cases, reveal indications of data protection infringements or discriminatory practices, which could prove useful in subsequent legal proceedings.[1407] However, the information provided is unlikely to include details that would be considered damning in legal proceedings, as employers determine the content[1408] and the GDPR appears to impose only limited specificity requirements.[1409]

The AIA also sets more specific informational safeguards regarding AI-supported decision-making that does not involve ADM, which could help patch over some of the gaps left by the GDPR. However, the AIA's safeguards are applicable only when high-

1401 (Publication III / Parviainen 2024, 459–60).
1402 Nevertheless, the likelihood that the job applicants read the privacy policies where the information is included is probably also low. See, e.g., (Auxier et al. 2019).
1403 See section 5.2.2 above.
1404 (WP29 2018a, 25).
1405 GDPR Arts. 13(2)(f) and 14(2)(g).
1406 C-203/22 *Dun & Bradstreet Austria,* para 58.
1407 (Publication III / Parviainen 2024, 459–60).
1408 (Busuioc et al. 2023, 86).
1409 (Metikoš 2025). See also (Rosin and Parviainen 2025, 488).

risk AI systems are used. 'Internal' job applicants seeking another position within the same organisation may be informed under AIA Article 26(7) also of the use of ARSs that do not assist in decision-making. This information could be given in information and consultation proceedings, making it potentially more nuanced and detailed than the other disclosures available for all job applicants. However, the scope of this safeguard is limited as it does not assist external job applicants.[1410]

Nevertheless, pursuant to AIA Article 26(11), all job applicants should be informed of the use of high-risk AI systems that assist in decision-making concerning them. This safeguard has a broader scope of application than the GDPR's ex ante information disclosures related to ADM, as it also applies when human recruiters are meaningfully involved in the recruitment decision-making process. Yet, it appears content-wise more limited than the GDPR's ADM disclosures. Namely, based on its wording, AIA Article 26(11) appears to require only disclosing the fact that a high-risk AI system is used in decision-making concerning job applicants. Nevertheless, AIA Recital 93 states that the information to be disclosed should also include the intended purpose of the system, the type of decisions to be made and information about the job applicants' right to an explanation under AIA.[1411] No details of the ARS or its effects must be shared.[1412] Accordingly, information to be provided under AIA Article 26(11) is unlikely to assist directly in enforcing data protection or non-discrimination provisions. However, after being informed of the ARSs, job applicants could be better prepared to actively seek further information by utilising the remaining informational safeguards discussed next.

6.1.2.2 Information accessible upon request

Regarding high-risk AI recruitment systems, job applicants could proactively seek more information about the system from the EU database of high-risk AI systems, assuming they are familiar with the database and have sufficient information to submit a query. Thus, from the perspective of job applicants, it would be important that information provided on the basis of AIA Article 26(11) would include information about the existence of the EU database for high-risk AI systems, as well as the system's and the provider's name, or other information potentially required for finding the system from the database.[1413]

1410 See also (Publication IV / Parviainen 2026).
1411 See AIA Recital 93.
1412 Cf. GDPR Arts. 13(2)(f) and 14(2)(g).
1413 However, these are not explicitly required in AIA Art. 26(11). See also (Publication IV / Parviainen 2026). As of November 2025, the database has not yet been set up, so the details of its functioning remain still unclear.

The information that high-risk AI system providers must publish in the public EU database for high-risk AI systems, pursuant to AIA Articles 49 and 71, could be more useful for job applicants in their enforcement actions than the automatically provided information.[1414] In the database, job applicants should find general information about the workings of the ARS, such as 'a basic and concise description of the information used by the system (data, inputs) and its operating logic'.[1415] Further, electronic instructions for use should also be included in the database.[1416] The electronic instructions for use could provide job applicants with more detailed information about the characteristics, capabilities, and performance limitations of the high-risk AI system than what they would receive from systems using ADM under GDPR Articles 13 and 14.[1417] While the EU database could be consulted without employer involvement, several other informational safeguards require direct contact with the employer.

The right of access under GDPR Article 15 is triggered only when job applicants exercise this right against the employer. In addition to the general information about the processing of personal data and potential ADM-specific disclosures, the right of access gives job applicants information about which of their personal data is processed, and they are also granted access to a copy of the personal data concerning them.[1418] GDPR Article 15(3) stipulates that only one copy of personal data must be provided free of charge, and for any further copies, the controller may charge a reasonable fee based on the administrative costs incurred. Thus, job applicants should consider the best time to utilise their right of access, as the GDPR does not restrict the timing.

Depending on the phase of the recruitment process in which the right of access is invoked, it might reveal only the data provided by the job applicant, data inferred from

1414 (Publication III / Parviainen 2024, 460) and (Publication IV / Parviainen 2026).

1415 AIA Annex VIII Section A, point (6).

1416 AIA Annex VIII Section A, point (12). Of the contents of the electronic instructions for use, see AIA Art. 13(3).

1417 (Publication IV / Parviainen 2026). See AIA Art. 13(3) according to which, for instance, information on the metrics, possibly risky circumstances, technical capabilities, characteristics and performance regarding specific groups should be included in the instructions for use.

1418 (EDPB 2023, 3). See also case C-579/21 *Pankki-S*, where the right of access was deemed to entitle data subjects to receive information also about the logs related to their personal data (i.e. dates and purposes of the consultation). In that case, however, information about the identity of the employees who had consulted the data was not to be provided unless essential for the effective exercise of rights. The rights and freedoms of those employees must also be considered when deciding on the right of access. For the Finnish Supreme Administrative Court's final ruling on the matter, see KHO:2025:51.

that original data or decisions made concerning the job applicants.[1419] Ensuring that personal data is correct before any decisions are made could help prevent inaccurate decisions. However, obtaining information about the decisions themselves could be crucial for challenging discriminatory outcomes.[1420] Even when no automated decisions are made, the inferences drawn about job applicants and disclosed upon exercising the right of access could reveal data protection breaches or discrimination. For instance, the inference could contain a protected ground unrelated to the job applicant, thereby revealing both the inaccuracy of the applicant's personal data and the possibly discriminatory nature of the ARS. If the right of access is exercised after an automated decision, it also encompasses a right to explanation, which will be examined next, together with its counterpart in the AIA.[1421]

Based on CJEU case law, GDPR Article 15(1)(h) establishes a right to an explanation of automated decisions that have legal effects or similarly significant effects on applicants.[1422] AIA Article 86 also establishes a right to an explanation, which applies to individual decision-making based on a high-risk AI system's output that produces legal effects or similarly significantly affects the job applicant in a way that they consider to have an adverse impact on their health, safety or fundamental rights. Although limited to high-risk AI systems and mainly adverse decisions[1423], the AIA's explanations could also be requested when humans make the final decisions,[1424] making them a potentially useful informational safeguard.[1425] To the extent that the scopes of the rights to explanations overlap, the GDPR takes precedence.[1426] Accordingly, ADM based on the processing of personal data should

1419 See also (EDPB 2023, 3).

1420 See case C-203/22 *Dun & Bradstreet Austria*, para 58.

1421 Of the comparisons of the two rights to explanation, see also (Metikoš and Ausloos 2025; Nisevic et al. 2024; Grozdanovski 2025)

1422 See case C-203/22 *Dun & Bradstreet Austria*, para 57.

1423 Explanations under the AIA must also be given for positive decisions that have legal effects, such as a decision to enter into an employment contract. As discussed in (Publication IV / Parviainen 2026) from an individual job applicant's perspective, the limitation to adverse decisions appears understandable, as these are the ones that typically require explanations to facilitate challenging and the utilisation of the remedial safeguards. However, from the perspective of job applicants as a collective, it could be useful to receive information about the positive decisions as well, as those may be needed as evidence in building discrimination claims.

1424 Of the human involvement in recruitment, see e.g., (ICO 2024, 32; Carter 2024, 351–52).

1425 For a comparison of the scopes of the rights, see also (Publication IV / Parviainen 2026) and (Brkan and Palčič Vilfan 2024, 1203–4; Grozdanovski 2025; Metikoš and Ausloos 2025).

1426 AIA Art. 86(3). See also (Publication IV / Parviainen 2026) and (Brkan and Palčič Vilfan 2024, 1203–4).

be explained as required by the GDPR. In contrast, explanations for decisions made by humans on the basis of high-risk AI systems' output are to be explained as stipulated in the AIA. However, it should be sufficient for job applicants just to inform the employer that they want to utilise their right to explanation without specifying the provision to which they refer.[1427] Thereafter, it should be for the employer to determine which of the rights to explanation apply and what information the explanations must include.

The rights to explanation are intended to facilitate the exercise of other rights, including the ability to contest (semi-)automated decisions.[1428] At best, the rights to explanation could provide job applicants with information about the ARS's workings, which they could use to lodge a complaint with the supervisory authorities[1429] or a claim in court.[1430] However, it will depend on the content of the explanations, and thus on the employers, how effectively the explanations facilitate enforcement actions. Currently, it remains ambiguous as to what kinds of explanations would fulfil the requirements of the GDPR or the AIA, and whether and how those might differ.[1431]

There are some differences in the wording of the rights to explanation.[1432] First, the type of information to be provided varies: the AIA demands that the information is clear and meaningful,[1433] whereas under the GDPR, the information must be concise, transparent, intelligible and in an easily accessible form.[1434] The CJEU has considered that disclosing the algorithm would not fulfil the GDPR's requirements.[1435] From the perspective of individual applicants, this emphasis on

1427 GDPR Art. 12 requires employers as controllers to facilitate the exercise of data subject rights, including the right to explanation.

1428 See AIA Recital 171. As regards GDPR, see C-203/22 *Dun & Bradstreet Austria,* para 58.

1429 Under AIA Art. 85, GDPR Art. 77 and potential national non-discrimination legislation.

1430 GDPR Arts. 78–79 and potential national non-discrimination legislation or tort law.

1431 Scholars have proposed varying interpretations. *Ljupcho Grozdanovski* argues that the GDPR's explanations could include 'knowledge about the rationale of automated output' while the AIA's explanations focus on 'human agent's reasons to rely on that system's output', (Grozdanovski 2025, 11–15). *Ljubiša Metikoš and Jef Ausloos* have considered that GDPR and the AIA grant similar types of explanations (Metikoš and Ausloos 2025, 223–29, 237).

1432 Under the GDPR, the right is not explicitly mentioned except for the Recital 71. The wording herein refers to the right of access (Art. 15) and the general provision of transparency and modalities for ensuring it (Art. 12), referred to also in the case of *Dun & Bradstreet Austria* (C-203/22).

1433 AIA Art. 86(1).

1434 GDPR Arts. 12–15 and C-203/22 *Dun & Bradstreet Austria,* paras 50 and 58.

1435 C-203/22 *Dun & Bradstreet Austria*, para 58. See also (Metikoš 2025).

accessibility is understandable, as they often lack the resources or technical capacity to investigate more complex disclosures. However, excluding more detailed explanations may prevent some more profound investigations into the ARSs' conduct by, for example, non-profit organisations or trade unions that may have or acquire the required resources and expertise.[1436]

The AIA's explanations might facilitate more in-depth explanations. At the structural level, the AIA's focus is generally broader, encompassing the operations of AI systems, rather than just the processing of personal data, as in the GDPR. This could imply that the clear and meaningful information under the AIA may be given a slightly different meaning in practice than for the GDPR's information requirements. Considering also that the AIA does not explicitly require conciseness or transparency of the explanations, the AIA's explanations could perhaps be more technical and more detailed.[1437] Nevertheless, at the level of the individual provisions on the right to explanation, the aims converge, as both seek to facilitate the exercise of rights. Accordingly, the purposes of the individual provisions suggest that there might not be considerable differences between the explanations.

Second, the wording on the contents of the rights to explanation appears to differ as well. GDPR Article 15(1)(h) demands disclosure of the existence of ADM, 'meaningful information about the logic involved' and the significance and envisaged consequences of such processing for the data subject. The CJEU has read this provision as requiring disclosure of the procedure and principles applied in the automated processing of personal data to achieve a specific result.[1438] The explanations could comprise concise, understandable information about, for example, the personal data used, the criteria considered, and their weights in the specific decision-making situation.[1439] AIA Article 86(1) demands informing of 'the role of the AI system in the decision-making procedure and the main elements of the decision taken'. Hence, job applicants should be informed of which part of the recruitment process the high-risk AI system handles, whether the decision-making is solely automated, and, if not, how human recruiters are involved.[1440] This information is not required in the GDPR, where the right to explanation applies only to ADM.[1441] However, the 'main elements of the decision taken' to be disclosed as

1436 See also (Metikoš 2025; Rosin and Parviainen 2025, 488).
1437 See also (Publication IV / Parviainen 2026).
1438 C-203/22 *Dun & Bradstreet Austria,* para 58.
1439 See, e.g., (Metikoš and Ausloos 2025, 223–27). For views prior to the Dun & Bradstreet judgement, see also (Wachter et al. 2017, 97; WP29 2018a, 25–26; Grozdanovski 2021, 123–24) and AG Pikamäe's opinion in C-634/21 *Schufa,* paras 54–58.
1440 (Publication IV / Parviainen 2026).
1441 (Publication IV / Parviainen 2026). Similar information could nevertheless be included in the description of the logic involved in ADM (GDPR Art. 15(1)(h)).

part of the AIA's explanations could be rather similar to the logic involved under the GDPR, comprising, among others, the types of algorithms used, their underlying logic, input and training data, outputs and the decision-making criteria utilised.[1442] Thus, despite the variations in the wording of AIA Article 86(1) and GDPR Article 15(1)(h), the informational content to be provided under the two rights to explanation might not differ significantly.[1443]

Nevertheless, it remains to be seen how the CJEU will interpret these rights to explanation. If the CJEU decides to interpret the contents of the rights to explanation divergently, granting job applicants more useful information under the AIA, its Article 86(3) should be interpreted teleologically, with due regard to the purpose of facilitating the exercise of rights. Under such an interpretation, job applicants should be provided with the additional information on the basis of AIA Article 86, even when the GDPR's right to explanation applies.[1444]

The rights to explanation also differ with regard to their enforceability. If the GDPR's right to an explanation is not complied with, the job applicant can complain to a data protection authority,[1445] bring a claim in court against the employer,[1446] and even seek compensation on the basis of the GDPR, if damages have occurred.[1447] The data protection authorities' investigation might also result in a considerable administrative fine.[1448] The existence of these remedial safeguards strengthens the GDPR's right to explanation. However, if an explanation is provided after a request, proving that it is insufficient in some regard is challenging, as the job applicants do not have access to the systems.[1449]

In contrast, under the AIA, the job applicant may only lodge a complaint with the market surveillance authority,[1450] which can then investigate the matter and use its powers under the AIA and the Market Surveillance Regulation. Yet, administrative fines are not a possible consequence for breaching the right to explanation under the AIA. Moreover, job applicants are not provided with any judicial remedies or rights to compensation under the AIA. Claims in court may be

1442 See AIA Art. 86(1) and (Brkan and Palčič Vilfan 2024, 1207). See also (Publication IV / Parviainen 2026).
1443 See also (Metikoš and Ausloos 2025, 223–29, 237).
1444 See also (Publication IV / Parviainen 2026) and AIA Art. 1 and Recital 9.
1445 GDPR Art. 77. See also GDPR Art. 78 allowing claims against data protection authorities' decisions in court.
1446 GDPR Art. 79.
1447 GDPR Art. 82.
1448 GDPR Art. 83.
1449 Yet, the case of *Dun & Bradstreet Austria* (C-203/22) is an example of such a contestation, so it is not impossible.
1450 AIA Art. 85.

possible under national legislation if the breach has caused damage to job applicants, but proving this could be difficult.

Although the explanations are a notable source of information, they should not be given too much weight.[1451] For instance, explaining the criteria used in the decision-making could, in some exceptional cases, reveal that protected grounds or proxies for those are used in making recruitment decisions. In such cases, the explanations could assist job applicants in lodging claims against employers. However, to the extent that indicia of discrimination or other non-compliance are intelligible to humans, employers are likely to avoid communicating them to job applicants.[1452] Given the ambiguity in the explanations, there could also be considerable variation in the usefulness of the information provided. Some explanations may be too technical, while others are overly simplistic, hindering further investigation into the workings of the ARSs. Furthermore, as discussed in Publication III, decisions could often be based on complex and unintelligible proxies that might remain undetected even if included in the explanations.[1453] Moreover, the right to explanation is not an absolute right and must be balanced against other rights and interests, including the protection of trade secrets.[1454] No true access to the system or visibility into its workings is offered to job applicants.[1455]

However, the AIA contains several provisions that could increase the amount of information available to supervisory authorities, thus enhancing public enforcement.[1456] As discussed in more detail in Publication IV, the AIA requires providers of high-risk AI systems to document and retain information on the design and development process, and to record their functioning.[1457] As a result, the supervisory authorities can have access to, for instance, technical

1451 The explanations are available only for automated decision-making or high-risk AI decision-assistance systems; ARSs supporting other stages in the recruitment process (e.g. drafting individualised job interview questions) may remain unexplained.

1452 Of the explanations as communication and the power it gives to those drafting the explanations, see, e.g., (Busuioc et al. 2023, 85–86).

1453 See, e.g., (Prince and Schwarcz 2020, 1304; Wachter 2022, 158–59; Publication III / Parviainen 2024, 443).

1454 GDPR Recital 63. See also C-230/22 *Dun & Bradstreet Austria*, para 76 and C-487/21 *Österreichische Datenschutzbehörde and CRIF*, paras 43–44.

1455 (Busuioc et al. 2023, 81). See also (Publication IV / Parviainen 2026). The supervisory authorities have direct access to the systems and the authority to test them, which could help address some shortcomings in the mediated communication provided to job applicants. However, without job applicants' complaints, such investigations are likely to be conducted only in the most severe and wide-ranging cases, given that authorities must allocate their limited resources effectively to the most significant matters.

1456 (Publication IV / Parviainen 2026).

1457 See AIA Chapter III, especially Section 2 and Articles 16–21.

documentation,[1458] logs,[1459] and quality management systems[1460] that might reveal some infringements.[1461] The documentation accessible to supervisory authorities could be more authentic, as it is not drafted by employers to be meaningful to the average job applicant. The logs could be even more authentic and unmediated, making them potentially useful in detecting breaches of data protection and discrimination.[1462] Furthermore, the AIA establishes reporting obligations for risks and incidents related to high-risk AI systems, which could result in more infringements being brought to the authorities' attention than under the GDPR's reporting requirements.[1463] Yet, if the authorities do not have the resources to investigate the systems further, the usefulness of this information and these reporting obligations is likely to be limited.

6.1.3 Remedial safeguards

In a legal framework where ex-ante external oversight is limited, remedial safeguards are crucial for ensuring the protection of job applicants. Remedial safeguards are ex-post reactive safeguards that offer means of redress when infringements occur.[1464] Traditionally, judicial remedies have been at the core of the remedies discussion. However, the EU digital legislation might indicate a shift in this regard, requiring specific internal remedial mechanisms as well.[1465] Thus, remedial safeguards are understood broadly to cover not only judicial remedies but also administrative remedies that may lead to independent decisions by supervisory

1458 AIA Art. 11 and Annex IV. The technical documentation should include a description of the AI system and its development, comprising information about the general logic of the system and the algorithms, what the system is designed to optimise for, parameters' relevance, training data sets used, assessment of human oversight measures, validation and testing procedures (e.g. metrics used to measure discriminatory impacts) and all the test logs and test reports.

1459 AIA Art. 12. The logs should allow traceability of the system, assisting in identifying situations that present risks.

1460 AIA Art. 17. The quality management systems could contain indicia of the provider's regulatory compliance measures.

1461 (Publication IV / Parviainen 2026).

1462 See also (Publication IV / Parviainen 2026).

1463 (Publication IV / Parviainen 2026). See AIA Arts. 20(2), 26(5) and 73. Cf. GDPR Art. 4, point (12), and Arts. 33 and 34.

1464 See, e.g., (Shavell 1993, 257–58; Suksi 2020, 4; Smuha 2024a, 254).

1465 For a broader approach to remedies under the EU digital legislation, see also (De Gregorio and Demkova 2024).

authorities[1466] and the internal remedial mechanisms established in the relevant EU legislation.[1467]

This subchapter begins by discussing the remedial mechanisms that employers must implement, and which job applicants can refer to if they suspect problems with the ARSs. These remedies have already been discussed in section 5.2.2, as it is the employer's duty to set them up. However, judicial and administrative remedies were not included in the framework of key legal parameters for ARS use, as they do not require active implementation by employers.[1468] Nevertheless, judicial and administrative remedies could at least have an indirect effect on the employer's compliance efforts, possibly targeting compliance measures to areas where the likelihood of successful enforcement actions is highest.

6.1.3.1 Remedies implemented by employers

The framework of key legal parameters includes several provisions that require employers to establish mechanisms to correct problems with the ARSs (i.e., internal remedies[1469]). The rights to rectification, erasure, restriction of processing, and objection can also be seen as remedial safeguards, as they aim to correct or end practices that have already breached data protection rights or could be likely to do so.[1470] Although rooted in data protection, the effective exercise of data subject rights could also support non-discriminatory processes, for example, by mitigating the risk of decisions being made based on irrelevant or inaccurate data.[1471] To utilise these rights, job applicants must contact the employer, which should have procedures in

1466 In a narrow reading of remedies, administrative remedies might not be included, as the supervisory authorities are not tribunals as referred to in CFREU Article 47. See, e.g., (Kotschy 2020b, 1135). For a broader view, see also (De Gregorio and Demkova 2024).

1467 For a similarly broad approach to remedies, see also (De Gregorio and Demkova 2024) and (Publication IV / Parviainen 2026).

1468 While employers' primary concern should be compliance with the relevant legal parameters, they would do well to remain aware of the remedies available to job applicants. Equally significant from the employer's perspective are the administrative fines that may be imposed under the AIA and the GDPR.

1469 See, e.g., (De Gregorio and Demkova 2024, 233–35).

1470 For example, in the case of exercising the right to object (GDPR Art. 21), no breach has necessarily taken place yet. However, not complying with the job applicants' request could breach their data protection rights unless the employer demonstrates compelling legitimate grounds overriding the interests, rights and freedoms of the data subject, or unless it is required for the establishment, exercise or defence of legal claims.

1471 As an example of a situation where processing of irrelevant personal data also contributed to finding discrimination, see case KKO:2015:41of the Finnish Supreme Court.

place to fulfil the request.[1472] Depending on the characteristics of the ARS, the employer may also encounter practical and technical difficulties in fulfilling, for example, the right to rectification and erasure.[1473] The effectiveness of the internal remedial safeguards that apply to all types of ARSs could also be limited, if the employer does not comply with the request and the job applicant is not willing to take the matter further by lodging a claim with supervisory authorities or, ultimately, bringing a claim to court.

GDPR Article 22(3) demands several remedial safeguards to be established, but only when ADM takes place. The right to obtain human intervention, express one's point of view, and contest the decision, required by GDPR Article 22(3), could be deemed to protect job applicants' personal data[1474], safeguard them against discriminatory effects[1475] and enhance their ability to challenge automated decisions. The specifics of these safeguards are left open in the GDPR. For instance, it is not clarified what the procedure with these safeguards should be or at which stage of the process they could be utilised. Thus, the right to obtain human intervention and to express one's point of view could, in theory, be invoked already before any decisions are made. However, these safeguards are discussed below mostly as post hoc remedies.[1476]

In line with the WP29 guidance, the human intervention safeguard implies that job applicants should have the option to request an authoritative and competent human[1477] to review the automated decision and, if necessary, change it.[1478] According to the WP29 guidelines, the review should comprise 'a thorough assessment of all the relevant data', which could also be provided by the data subject

1472 Especially when the ARS is not making automated decisions or is not a high-risk AI recruitment systems assisting in decision-making, and there is no obligation to disclose additional data about the processing, it could be difficult for the job applicants to analyse whether the profiles made about them are correct and to show that those would require rectification.

1473 For instance, rectifying LLM-based recruitment systems' confabulations could be difficult in practice, see sections 5.2.2 and 6.2.

1474 GDPR Recital 71 implies that the measures aim to ensure fair and transparent processing of personal data, correction of inaccuracies in personal data and minimisation of risks.

1475 See GDPR Recital 71. See also AG Pikamäe's Opinion in case C-634/21 *Schufa*, para 19.

1476 See also (Almada 2019, 7).

1477 The more complex the ARS, the harder it is to review its decisions, possibly increasing also the risk of automation bias among human reviewers. For instance, in a global study of more than 48.000 respondents from 47 countries, two in three respondents admitted relying on AI output without evaluating the information it provides. See (Gillespie et al. 2025, 6).

1478 (WP29 2018a, 27). See also (Malgieri 2019, 22). This resembles the requirements of humans overseeing high-risk AI systems under the AIA Art. 26(2) and 14.

based on their right to express opinions.[1479] Nevertheless, there are no specific criteria in the GDPR against which the decisions should be reviewed, nor are there particular steps which the review must follow.[1480] In practice, the reviewers could be left to check whether the decision appears lawful and complies with the employers' policies, including recruitment criteria. As regards lawfulness, the reviewers should ensure that the decision does not discriminate. If the human reviewer upholds a discriminatory decision, personal liability may also arise, for instance, if the decision constitutes punishable discrimination under national criminal law.[1481] In addition to the decision-making criteria, the reviewer may be able to assess whether the decision was based on relevant and up-to-date personal data, which is also crucial for reaching accurate decisions. Moreover, the human reviewer might assess whether the process has fulfilled the transparency requirements of the GDPR and the AIA.

Yet the review is conducted by a representative of the employer, and the right to human review does not guarantee job applicants any alteration of the outcome of the decision-making. Should the job applicant deem the human review insufficient, they could lodge a complaint with the data protection authorities or ultimately bring a claim to court. However, based on the GDPR, the data protection authorities do not have the power to consider anything other than data protection issues.[1482] Whereas, if the applicants suspect discrimination, they should complain to equality bodies and ultimately to courts, as stipulated in national legislation. In a potential court case, breaches of the GDPR and related compensation claims could also be pursued.

Compared to human review, the right to express their point of view, as outlined in GDPR Article 22(3), appears even less effective, although it could be subject to the same enforcement and redress mechanisms just discussed. Essentially, the right to express their point of view gives job applicants the opportunity to explain why they think the decision is, for instance, biased, wrong, or inaccurate.[1483] However, the GDPR does not state how opinions should be noted in practice.[1484] If the opinion is presented before the human intervention, it can be taken into account in the review. Yet the GDPR appears to leave it to controllers to decide what role the opinions will play. The better grounded the opinions are, the more likely they are to affect, for instance, the review of the decision-making. The information provided, based on the right to explanation, could assist job applicants in forming compelling opinions that

1479 (WP29 2018a, 27).
1480 See also (Dreyer and Schulz 2019, 27).
1481 See, e.g., Finnish Criminal Code Chapter 47 Section 3.
1482 GDPR Art. 77. Breaching the safeguards established in GDPR Art. 22(3) could lead to administrative fines for the employers under GDPR Art. 83(5). However, it is possible that DPAs are also assigned the role of market surveillance authorities under the AIA.
1483 See also (Malgieri 2019, 22).
1484 See also (Brkan 2019a, 108).

may lead to amendments in the decisions. Nevertheless, this right may primarily serve as a symbolic safeguard, providing an avenue for expressing dissatisfaction rather than offering redress.[1485]

Additionally, GDPR Article 22(3) establishes a right to contest the decision. However, the contents of this right are not defined. The GDPR does not explain the procedure for contestation, its possible grounds, or its potential consequences. The right to contest the decision is mentioned separately from the right to human intervention; however, the contestation often coincides with the request for human intervention, so that the human reviewer will also handle the contestations.[1486]

The grounds for contestation are not determined in GDPR Article 22(3) either. Consequently, job applicants could contest the decisions based on arguments deriving from various legal instruments.[1487] For instance, in relation to the GDPR, job applicants could claim that the decision is based on incorrect or incomplete input data or that the data protection principles, such as fairness, have not been followed in ADM. Such a contestation might, at best, lead to making the decision anew on the basis of corrected or more limited data. However, the GDPR does not provide a means for contesting the decision-making criteria. Instead, the reasoning or decision-making criteria could be contested on the basis of the non-discrimination legislation.[1488]

Furthermore, the consequences of contestation remain undefined. GDPR Article 12(3) only requires that information on the action taken must be provided without undue delay and, in any event, within one month of the request.[1489] GDPR Article 12(4) confirms that it is also an option not to take action, as long as the reasons for such a decision are provided to the data subject and they are informed of the possibility to lodge a complaint with supervisory authorities and to seek a judicial remedy. Hence, the results of cases where job applicants' contest decisions could vary significantly, and controllers retain broad discretion. In an ideal scenario from the job applicant's perspective, the employer would rectify the problematic decision directly, without the need to resort to judicial or administrative remedies. In a more realistic scenario, there

1485 Cf. (Malgieri 2019, 21–22).

1486 See also (Malgieri 2019, 22). However, the GDPR does not appear to categorically exclude machine-handled contestations where human intervention has not been requested. Nevertheless, any decision produced by such a process could itself constitute ADM, meaning the job applicant could utilise the same safeguards in relation to that decision. Accordingly, the practical value of allowing machines to handle contestations in the first place may be limited.

1487 Nothing prevents job applicants from using non-legal arguments. Some ethical arguments may also prompt certain employers to reconsider their decisions, even if there is no legal obligation to do so.

1488 See (Wachter and Mittelstadt 2019, 571) and the case C-434/16 *Nowak*.

1489 For further details of the timing and requirements GDPR sets for the process, see GDPR Art. 12.

might be no amendments to the procedure followed or the decisions made. If the job applicant is unhappy with the procedure or the results of the contestation, they can complain to data protection authorities or bring a claim to court against the employer, alleging breaches of the GDPR or the non-discrimination legislation.

6.1.3.2 Judicial and administrative remedies

As the preceding discussion of preventive, informational, and internal remedial safeguards has implied, the effectiveness of these safeguards often depends on the ability to enforce them through administrative and judicial procedures. There are certain remedial safeguards established directly in the EU legislation, such as the rights to judicial remedies under the GDPR[1490] and the rights to lodge complaints with supervisory authorities under both the GDPR[1491] and the AIA[1492]. The Non-Discrimination Directives also envision certain safeguards, though these are implemented through national legislation. This section focuses on the remedial safeguards established at the EU level, which are compiled in Table 2 below.[1493]

	GDPR	AIA	Non-Discrimination Directives
Judicial remedies	Right to an effective judicial remedy against: 1) a supervisory authority's legally binding decision concerning them, or neglect of handling a complaint, or informing of its progress (GDPR Art. 78); and 2) a controller or processor when rights under the GDPR are infringed as a result of non-compliant personal data processing (GDPR Art. 79).	-	Member States to determine: judicial procedures for the enforcement of obligations under the Non-Dicrimination Directives must be available to all persons who consider themselves wronged by failure to apply the principle of equal treatment to them (GED Art. 17(1) – explicit requirement, EED Art. 9(1) and RED Art. 7(1) as read in light of CFREU Art. 47).

1490 GDPR Arts. 78 and 79.
1491 GDPR Art. 77.
1492 AIA Art. 85.
1493 However, there may be criminal law sanctions in the national legislation targeted both at the employer organisation and employees utilising the ARSs on behalf of the employer, among other issues, for severe data protection breaches and discrimination. For instance, in Finland, both severe data breaches and discrimination could lead to criminal sanctions under the Criminal Code (39/1889).

	GDPR	AIA	Non-Discrimination Directives
Administrative remedies	Right to lodge a complaint with supervisory authority where processing of their personal data infringes the GDPR (GDPR Art. 77).	Right to lodge a complaint with a market surveillance authority for infringements of the AIA (AIA Art. 85).	Member, States to determine: recourse to competent authorities, including appropriate conciliation procedures may be offered (GED Art. 17(1), EED Art. 9(1) and RED Art. 7(1)).
Potential form of redress	In claims against employers: compensation for the material or non-material damage suffered as a result of a GDPR infringement (GDPR Art. 82).	-	Member States to determine: sanctions may comprise the payment of compensation or reparation to the victim, and must be effective, proportionate and dissuasive (EED Art. 17, RED Art. 15, GED Art. 18).
			Compensation or reparation may not be restricted by fixing a prior upper limit, except where the employer proves that the only damage suffered is the refusal to consider a job application (GED Art. 18).

Table 2. Judicial and administrative remedies available to job applicants under EU law.

The remedial safeguards must be assessed against the standard set by CFREU Article 47, which establishes a right to an effective remedy before a tribunal for everyone who considers that their rights under EU law have been violated. The CFREU Article 47 also requires that procedural safeguards[1494] and necessary legal aid are secured. The right to an effective remedy means that pursuing EU-law-based claims must not be 'practically impossible or excessively difficult'.[1495] While the impossibility standard appears to refer to objective factors,[1496] the assessment of

1494 CFREU Art. 47(2) requires fair and public hearings within a reasonable time, independent and impartial tribunals and a possibility for legal representation to be guaranteed.

1495 C-268/06 *Impact*, para 46, and (Bobek 2014, 167).

1496 For instance, case C-362/14 *Schrems* provides an example of impossibility, where the legislation did not provide any possibility for an individual to pursue legal remedies to have access to personal data or obtain rectification or erasure of such data (para 95).

excessive difficulty may also take into account more subjective factors.[1497] For instance, the job applicants' ability to access evidence necessary to substantiate their claims could be noted when assessing the effectiveness of the remedies available.[1498]

In the absence of EU procedural rules, the details of the procedures are left for the Member States to decide, and significant national differences in the practical implementation of the remedial safeguards may arise.[1499] Member States must nevertheless ensure that their procedural rules neither hinder the practical application of EU law nor apply less favourable standards to EU-related cases than to comparable domestic ones.[1500] Eventually, Member States bear the responsibility for ensuring that remedial procedures are effective in practice.[1501]

The scope of the remedial safeguards appears to be rather broad based on EU legislation. The GDPR's judicial and/or administrative remedies could apply to all ARSs that process personal data. The remedies established on the basis of the Non-Discrimination Directives could also be applicable regardless of the type of ARS. Further, the administrative remedies under the AIA also apply to all types of AI systems. Hence, there should be some remedial safeguard, either judicial or administrative, available for job applicants regarding each of the preventive, informational, and internal remedial safeguards discussed above. However, their usefulness to individual job applicants varies.

For individual job applicants, the strongest remedial safeguards could be the judicial remedies that could lead to an award of compensation, provided that utilising these remedies is practicable. At the EU level, the right to compensation is ensured only based on GDPR Article 82, which can be claimed in the judicial procedures envisaged in GDPR Article 79.[1502] Nevertheless, in non-discrimination law, rights to compensation can be established at the national level, where the alleviation of the burden of proof could facilitate the pursuit of this compensation. The weakest situation appears to be with the AIA, as there is no right to compensation for damaging breaches of the AIA.[1503]

1497 (Bobek 2014, 167).
1498 See also (Publication III / Parviainen 2024, 463–64).
1499 See cases C-33/76 *Rewe*, para 5 and C-45/76 *Comet*, para 13. See also (Lenaerts et al. 2023, 119–20).
1500 See cases C-33/76 *Rewe*, para 5 and C-45/76 *Comet*, para 13.
1501 TEU Art. 19(1). See also cases C-33/76 *Rewe,* para 5 and C-222/84 *Johnston,* paras 17-20. For discussion of the CFREU Art. 47, especially on the employment context, see (Adams-Prassl 2020).
1502 However, as Kotschy has pointed out, the compensation claims against controllers (GDPR Art. 79) might coincide with the claims against the decisions of supervisory authorities (GDPR Art. 78), depending on the national implementation. See (Kotschy 2020b, 1140).
1503 See also (Publication IV / Parviainen 2026).

The GDPR's judicial remedies, established in Article 79, grant data subjects (i.e., job applicants) a right to an effective judicial remedy against a controller or processor when they consider that their rights under the GDPR have been infringed as a consequence of the processing of their personal data in a manner that is non-compliant with the GDPR.[1504] This right is important, as it offers job applicants an avenue for claiming compensation under GDPR Article 82, since supervisory authorities lack the power to order compensation to be paid.[1505] Although GDPR Article 79 specifies certain details, such as territorial and representational aspects, job applicants must check national legislation on how judicial remedies are to be utilised in practice.

Some general directions regarding the burden of proof may also be found in the wording of GDPR Article 82 and its accountability-related provisions,[1506] although the GDPR does not explicitly specify the burden of proof.[1507] Pursuant to GDPR Article 82(1) 'any person who has suffered material or non-material damage as a result of an infringement of' the GDPR has the right to receive compensation for the damage suffered from the controller or processor. Considering the dual objectives of the GDPR,[1508] the CJEU has interpreted this provision to provide 'for a fault-based liability in which the burden of proof rests not on the person who has suffered damage, but on the controller'.[1509] Accordingly, the employer's fault is presumed unless it proves that it is not responsible in any way for the event giving rise to the damage.[1510] Nevertheless, in order to raise a claim for compensation in court, a job applicant should be able to demonstrate that: (i) the employer has, in some way, breached the GDPR; (ii) they have suffered material or non-material damage; and (iii) there is a causal link between the infringement and the damage

1504 Thus, the GDPR actually appears to reiterate the CFREU Art. 47, highlighting that a right to an effective remedy must exist in all situations, even when administrative or non-judicial remedies are also in place (Kotschy 2020b, 1135–36).

1505 See GDPR Art. 58. See also (Kotschy 2020b, 1135).

1506 GDPR Art. 5(2) requires that the controller is responsible for, and able to demonstrate compliance with the principles of processing personal data. In addition, GDPR Art. 24(1) requires appropriate technical and organisational measures to ensure and demonstrate that the processing complies with the GDPR. Similarly, also in GDPR Art. 7(1) on the existence of consent and Art. 11(2) and 12(2) on the data subject's identifiability. See also (Van Alsenoy 2016, 282; De Hert et al. 2013, 141).

1507 See also (Van Alsenoy 2016, 282–83). In contrast, see EED Art. 10, RED Art. 8 and GED Art. 19. The standard rules of evidence require the party alleging something to prove it (Koukiadaki 2024, 637–38), which is often difficult for job applicants, also in traditional recruitment cases, not to speak of algorithmic recruitment.

1508 See GDPR Recitals 4 and 8 and section 1.3.3 above.

1509 See, e.g., C-667/21 *Krankenversicherung Nordrhein,* para 94.

1510 GDPR Art. 82(1) and (3). See also C-655/23 *Quirin Privatbank*, para 71 and (Zanfir-Fortuna 2020, 1176).

suffered.[1511] Considering the job applicants' limited access to information and employers' greater ability to provide evidence of their compliance measures, the job applicants should not be required to present detailed information on exactly where the processing has breached the GDPR.[1512] For instance, *Brendan Van Alsenoy* has argued that, de facto, it could suffice for data subjects to provide prima facie evidence of unlawful processing.[1513]

GDPR Article 82 provides for a right to compensation for both material and non-material damage. This financial compensation should fully compensate for the damage actually suffered as a result of the GDPR infringement, but it does not serve a punitive function.[1514] Since non-material damages are also to be compensated, for instance, damage to reputation arising from confabulations by LLM-based recruitment systems could be compensated under GDPR Article 82 if the system was deemed to have breached the principles of processing personal data.[1515] The compensation payable under GDPR Article 82 is to be assessed under Member States internal rules, noting the principles of equivalence and effectiveness of EU law.[1516]

However, the GDPR's remedies are limited to data protection infringements, and job applicants' possibilities to challenge the outcomes are limited in purely data protection-based cases.[1517] For example, basing a recruitment decision on inaccurate data could result in hiring a less qualified applicant. If the job applicant contests the decision, claiming that it was made on the basis of inaccurate personal data, the result under the GDPR could be compensation and correction of the personal data, but not typically a change in the recruitment decision itself.[1518] If the grounds for decision-

1511 See, e.g., C-655/23 *Quirin Privatbank*, para 56, C-300/21 *Österreichische Post*, paras 32-33, 37 and 42, and C-507/23 *Patērētāju tiesību aizsardzības centrs*, paras 24-25.

1512 See also (Van Alsenoy 2016, 283; De Hert et al. 2013, 141).

1513 (Van Alsenoy 2016, 283).

1514 See GDPR Recital 146 and cases C-667/21 *Krankenversicherung Nordrhein,* para 84–87 and C-687/21 *MediaMarktSaturn,* para 50. The employer's fault may not affect the amount of damages either, see, e.g., C-655/23 *Quirin Privatbank*, paras 69-70 and C-300/21 *Österreichische Post*, paras 57–58.

1515 The non-material damage may, according to GDPR Recitals 75 and 85, include damage to reputation or discrimination. Furthermore, there are no limits regarding the degree of seriousness of the damage, see, e.g., C-300/21 *Österreichische Post*, para 51 and C-200/23 *Agentsia po vpisvaniyata,* paras 147 and 149. Even negative feelings, such as fear or annoyance, may count as non-material damage giving rise to compensation, if the causal link between the breach of the GDPR and the feelings is proven, see C-655/23 *Quirin Privatbank*, para 62.

1516 See cases C-667/21 *Krankenversicherung Nordrhein,* paras 83 and 101 and C-687/21 *MediaMarkt Saturn,* para 53.

1517 See also (Wachter and Mittelstadt 2019, 571).

1518 See GDPR Arts. 16 and 82. See also (Wachter and Mittelstadt 2019, 571).

making appear discriminatory, they would have to be contested under non-discrimination legislation.

The Non-Discrimination Directives require Member States to ensure that judicial and/or administrative procedures for enforcing the directives' obligations are available to all persons who consider that the principle of equal treatment has not been applied to them.[1519] While the GED always requires a judicial procedure to be available,[1520] under the EED and the RED, a literal reading would make the judicial procedure optional and possibly replaceable by an administrative procedure.[1521] However, under CFREU Article 47, even if the first-instance remedy is administrative, Member States should, at a minimum, offer judicial review of the administrative decision to ensure an effective remedy is in place.[1522] Yet, the details are left to the Member States to decide, which could lead to significant differences in protection across the EU.[1523]

The Non-Discrimination Directives explicitly alleviate the burden of proof. Namely, the allegedly discriminated persons must only establish 'facts from which it may be presumed that there has been direct or indirect discrimination' to shift the burden of proof to the respondent.[1524] The evidential threshold required to trigger this shift could significantly affect job applicants' protection against discriminatory ARSs. However, as discussed in more detail in Publication III, even this reduced evidentiary standard could be challenging to meet in cases involving complex ARSs.[1525]

The sanctions applicable to infringements of national non-discrimination legislation are also left to the Member States' discretion, as long as those are effective, proportionate, and dissuasive.[1526] Purely symbolic sanctions are not

[1519] EED Art. 9(1), RED Art. 7(1) and GED Art. 17(1). *Chopin and Germaine* have found in their comparative study of the national non-discrimination legislation that in most Member States judicial proceedings, whether civil, criminal, labour and/or administrative, are combined with non-judicial proceedings such as mediation or conciliation. Of the available procedures in Member States, see (Chopin and Germaine 2023, 83–85).

[1520] GED Art. 17(1).

[1521] EED Art. 9(1) and RED Art. 7(1). These instruments require 'judicial and/or administrative procedures, including, where they deem it appropriate, conciliation procedures'.

[1522] The supervisory authorities are not tribunals as referred to in CFREU Art. 47, see also (Kotschy 2020b, 1135).

[1523] See, e.g., (Chopin and Germaine 2023, 83–106).

[1524] See EED Art. 10, RED Art. 8 and GED Art. 19. For more detailed discussion on this, see also (Publication III / Parviainen 2024, 455–66).

[1525] See (Publication III / Parviainen 2024, 456–64). See also section 6.2 below.

[1526] GED Art. 18, RED Art. 15 and EED Art. 17. Of the range of national sanctions utilised, see, e.g., (Chopin and Germaine 2023, 102–6).

sufficient.[1527] Rather, the CJEU has deemed that the 'severity of sanctions must be commensurate to the seriousness of the breaches for which they are imposed, […] ensuring a genuinely dissuasive effective […] while respecting the general principle of proportionality'.[1528] The Non-Discrimination Directives mention compensation paid to the victim as one possible sanction, and do not provide the discriminated job applicant a right to be employed in the position in question.[1529] Hence, it appears that unless Member States have developed broader sanctions in their national legislation, the best such job applicants could receive would be compensation for the loss or damage caused by the discrimination.[1530]

Where compensation is provided as a sanction in national legislation, it must be adequate in relation to the damage suffered and may not be only nominal.[1531] In cases where the job applicant would not, in any case, have obtained the position due to the chosen applicant's superior qualifications, there may be an upper limit for the compensation payable.[1532] Assessing the damage in a recruitment situation can be difficult, as it often relies on several assumptions, such as the length of the employment relationship had it been established, and the duration of possible further unemployment. Moreover, if the job applicant has found employment but in a more precarious position, it could be challenging to determine compensation for this instability and for the efforts the applicant has made to secure the other position. The compensation could also be awarded only upon contestation, which creates a considerable legal cost risk that few job applicants may be able to bear.[1533] Further, legal proceedings may pose a risk to a job applicant's reputation. These risk factors are unlikely to be taken fully into account when determining the amount of compensation.

As the AIA does not provide for any effective judicial remedies for persons affected by AI systems to be used against the operators, job applicants must resort to other legislation if they deem that they have suffered damage as a result of the use of an AI recruitment system. In case the damage results from something other than discrimination or a breach of the GDPR, national tort law could be the last resort for job applicants. However, AI and algorithmic systems pose special challenges under

1527 C-81/12 *Asociaţia Accept*, para 64.
1528 See C-81/12 *Asociaţia Accept*, para 63 and the case law cited.
1529 However, particularly in recruitment discrimination cases upper limits for sanctions may also be imposed, see, e.g., GED Art. 18.
1530 GED Art. 18, RED Art. 15 and EED Art. 17.
1531 See also C-14/83 *von Colson and Kamann*, paras 23–24 and C-180/95 *Draehmpaehl*, para 25.
1532 See, e.g., C-180/95 *Draehmpaehl*, paras 33–35 and 37. See also GED Art. 18.
1533 (Chopin and Germaine 2023, 85–86).

tort law that can make it difficult for job applicants to obtain compensation.[1534] The situation could have been somewhat better for job applicants had the AI Liability Directive been adopted, as it would have enhanced their possibilities to request disclosure of evidence and somewhat alleviated their burden of proof.[1535]

In addition to judicial remedies, administrative remedies are also available under the GDPR and the AIA. Complaints to supervisory authorities under GDPR Article 77 or AIA Article 85, and claims against the data protection authorities' decisions under GDPR Article 78[1536] could be important avenues for investigating whether the preventive, informational, and internal remedial safeguards have been complied with.[1537] The authorities' resources for investigating the processing of personal data are typically more extensive than those of individual applicants, which emphasises the significance of administrative remedies. The administrative procedures could also be less burdensome for job applicants than a court claim, as they may require less time and effort and be less costly.[1538]

Although the administrative remedies do not provide direct compensation to job applicants, the administrative proceedings could result in multiple measures against the employer, including administrative fines, thereby enhancing the safeguards' preventive effects.[1539] For instance, under the AIA, the investigations might result in corrective actions ending the ARS's non-compliance, prohibitions or restrictions of ARS's dissemination, withdrawal or recall, or penalties for the operators.[1540] These measures could prevent the violations from continuing. Furthermore, the administrative procedures may facilitate judicial remedies by providing evidence of

1534 (Expert Group on Liability and New Technologies - New Technologies Formation 2019, 19–30). For instance, the type of damage caused by the ARS might not be compensable, and the causal link and fault could be difficult to prove.

1535 The Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (COM(2022)496 final 2022/0303 (COD) (hereinafter AILD or AI Liability Directive) could have offered more remedies in this regard, such as a right to request disclosure of evidence, but the Commission decided to withdraw it in its work programme for year 2025, (European Commission 2025a, 26). See also (Grozdanovski 2025, 21–22) and (Publication IV / Parviainen 2026).

1536 Cf. If job applicants are unhappy with the market surveillance authorities' decisions, the AIA does not provide any means to challenge them, so the applicants' remedies therefore depend on national legislation.

1537 For a more detailed discussion on the differences between the administrative remedial procedures under the GDPR and the AIA, see (Publication IV / Parviainen 2026).

1538 Similarly also (Kotschy 2020b, 1136).

1539 See GDPR Arts. 58 and 83 and AIA Arts. 99 and 70, as well as Market Surveillance Regulation Art. 14. However, the likelihood of fines remains rather modest. In 2025, noyb analysed EDPB statistics, finding that on average 1.3% of cases before data protection authorities resulted in a fine (noyb 2025).

1540 See Art. 14(4) of the Market Surveillance Regulation and AIA Arts. 79 and 99.

non-compliance, which job applicants can use in their claims against employers. However, job applicants might not receive as much information about the administrative proceedings under the AIA as they would under the GDPR, which could limit the evidence available through market surveillance authorities' investigations.[1541] Since the Member States may decide on the time limits for bringing a case as they deem appropriate,[1542] it is possible that the time limit passes before the administrative proceedings are completed, limiting the usefulness of administrative proceedings as a means to gather evidence.

While there appear to be some judicial and/or administrative remedies in place for cases where ARSs infringe job applicants' data protection or discriminate against them, those could be difficult to rely on in practice. Especially, in cases where the ARS does not involve ADM or high-risk AI decision-support, the job applicants would be entitled to limited information, which makes contesting the ARS use difficult. Even in the best-case scenario, job applicants could receive only compensation for the damage caused by data protection infringements and discrimination, and not get the job, which they may be deprived of due to these infringements. Given the significant demands of judicial proceedings in terms of time, financial cost, and technical expertise, combined with the likely low probability of securing only modest compensation and conceivable risks of negative impressions among prospective employers, utilising the remedial safeguards does not appear tempting.[1543]

The next subchapter will continue with the analysis of the shortcomings of the legal safeguards.

6.2 Shortcomings of the legal safeguards

As the previous discussion has implied, although the EU legislation establishes several legal safeguards to protect job applicants against breaches of their rights to data protection and non-discrimination, there appear to be several shortcomings. The main shortcomings identified in this dissertation relate to: (1) the vague preventive

[1541] The claimants' role in the procedure is also more minor, and the AIA does not oblige market surveillance authorities to inform claimants of the procedure. Instead, under the GDPR Art. 77(2), the supervisory authority must also inform the complainant how the matter progresses and what the outcome is. The AIA Art. 78 confidentiality obligations might further limit the information available to job applicants. See also (Busuioc et al. 2023, 97).

[1542] Of the national time limits in bringing discrimination cases, see (Chopin and Germaine 2023, 86–87).

[1543] Of these kinds of problems in discrimination cases in general, see (Chopin and Germaine 2023, 85–87). *Steven Shavell* has also discussed the incentives of private individuals to report non-compliance, while noting also the fear of reprisal as a limiting factor (Shavell 1993, 266–68).

safeguards, the compliance with which faces technical difficulties, (2) limited ex-ante and continuous external oversight mechanisms, (3) job applicants' challenges in detecting infringements within ARSs and proving those in court, and (4) the inherent limitations of available remedies.

Previous studies have indicated that LLM-based systems could further exacerbate some of the problems with legal safeguards.[1544] Hence, this subchapter discusses the shortcomings through a case study of an LLM-based recruitment system, which refers to a system built on a general-purpose base model and fine-tuned for specific recruitment tasks.[1545] LLM-based recruitment systems are intractable, meaning they are difficult to understand, analyse, predict, control, and challenge due to their complexity, uninterpretability, indeterminacy, and emergent, unpredictable behaviour.[1546] Accordingly, for instance, knowing and investigating how and why LLM-based recruitment systems work is extremely challenging, and even the developers may be unaware of some of the system's unanticipated capabilities.[1547] Nevertheless, LLM-based recruitment systems are, as a rule, subject to all the same safeguards as other high-risk AI recruitment systems.

The first shortcoming is that the legal safeguards are often vaguely formulated and potentially difficult to comply with. While the vagueness of the safeguards could, in principle, ensure their applicability to novel technologies, it also leaves considerable discretion to employers. Employers may struggle to determine what the legal safeguards require in practice or to interpret them in a way that privileges business considerations over job applicants' rights.[1548] While the vagueness and resulting weaknesses of the legal safeguards concern all ARSs, technical difficulties complicate compliance with the preventive safeguards, particularly for the more complex ARSs.

Employers' and even ARS providers' possibilities to prevent discrimination and data protection infringements could apparently be limited, especially with the intractable LLM-based recruitment systems. The increased indeterminacy and unpredictability of these models complicate testing and simulation efforts, which

1544 See, e.g., (Hacker et al. 2025, 3; Bommasani et al. 2021, 1 and 105–7).

1545 See section 3.3.2 above.

1546 See sections 3.3 and 3.4 above. The agentic AI recruitment systems can also utilise LLMs. Thus, these considerations could also be relevant in the context of such agentic AI recruitment systems. However, due to the increased autonomy of agentic AI systems, EU legislation could struggle even more to effectively regulate agentic AI recruitment systems.

1547 Of this tendency in LLMs see (Ohm 2024, 238–39; Bowman 2023, 8; Wei et al. 2023; Bommasani et al. 2021, 1 and 6; Hacker et al. 2025, 3) However, as *Pauline Kim* has pointed out, the previous generation of ARSs could also conceal the reasons for their decisions and detecting errors from those was arduous (Kim 2017, 857).

1548 See sections 5.2 and 5.3 above.

might otherwise have assisted experts in understanding and predicting other complex, uninterpretable models and preventing discrimination within such models.[1549] Thus, the intractability of LLM-based systems increases the risk that prohibited practices and rights infringements will remain undetected despite employers' efforts to comply with the preventive safeguards.

Further, there are certain known characteristics of LLM-based recruitment systems that could have data protection-infringing and discriminatory effects, which cannot be eliminated.[1550] Namely, LLM-based recruitment systems exhibit the well-known tendency to generate confabulations, that is, seemingly plausible but nonfactual content that may also contain personal data.[1551] Although the problem is known, the humans overseeing the systems might not be reasonably able to detect all the fabricated content. For instance, if the ARS creates summaries of video interviews, the human reviewer would have to review all the videos to detect and correct inaccuracies. Thus, decisions could be made on the basis of inaccurate personal data, and in the worst case, this might also lead to discrimination.[1552] Similar problems with inaccurate personal data also arise in more traditional profiling practices, but confabulations might take this to a whole new level because of their unpredictability.[1553] The confabulations could also question the effectiveness of job applicants' right to rectification as a remedial safeguard.[1554] Even if one confabulated data point is corrected, a new confabulation could arise in the next run of the system.

Preventive safeguards that require human oversight or intervention can also be challenging to implement effectively. The intractability of LLM-based recruitment systems could increase the level of knowledge and competence required of the persons responsible for monitoring them. Moreover, the potentially emergent behaviours of these systems also underscore the need for continuous training and upskilling of individuals involved in their operation and use.[1555]

1549 (Viljanen 2022, 316–19; Zollo et al. 2024).
1550 Of a practical case of confabulations, see, e.g., (noyb 2024).
1551 See section 3.3.2 above and (Huang et al. 2024, 2; OECD 2023, 10; Novelli et al. 2024, 13). At the moment, confabulations are a persisting problem of generative AI, see (Hacker et al. 2025, 1). Several factors in the LLM lifecycle could cause confabulations, and it has been debated whether those can ever be removed (Huang et al. 2024, 2–4; Banerjee et al. 2024, 1). Some techniques, such as RAG, have been offered as a solution to limit confabulations, see, e.g., (IBM Research 2023).
1552 See, e.g., (noyb 2024).
1553 (Engel et al. 2023, 3; Hacker et al. 2025, 17). Where errors arise in traditional profiles based on job applicants' personal data, the source of the inaccuracy may be more easily identifiable than in confabulated content, where no clear source is likely to exist.
1554 See, e.g., (noyb 2024).
1555 AIA Arts. 4, 26(2) and 14.

Automation bias[1556] is a notable risk across all types of ARSs, and it may be exacerbated in LLM-based recruitment systems that produce progressively credible and persuasive outputs.[1557] Automation bias could exacerbate, for instance, the harmful consequences of confabulations or heighten the risk of ADM use without employers' awareness.[1558] This risk may lead employers to disregard the lawful basis for ADM under GDPR Article 22(2) and to neglect the safeguards to be established under GDPR Article 22(3), thereby creating significant exposure to data protection violations and leaving potentially discriminatory outcomes undetected. The use of ADM, which employers did not anticipate, also limits job applicants' access to remedies, as they are neither informed of the ADM nor provided with any explanation of the decisions.

The problems that the vagueness of the preventive safeguards and the complexity of compliance cause are exacerbated by the limited external oversight. Accordingly, the second shortcoming concerns the limited ex-ante and continuous external oversight mechanisms.[1559] As regards ex-ante external oversight, DPIAs might lead to consulting data protection authorities if processing within the ARS poses a high risk to job applicants and the employer's measures have not mitigated this risk.[1560] For instance, when using LLM-based recruitment systems, the risk of confabulations may require consulting data protection authorities, since such errors could cause some job applicants to lose a job opportunity, and the confabulations cannot be fully mitigated. However, employers determine whether prior consultation with data protection authorities is needed.[1561] Thus, prior consultations may remain rare in practice.[1562]

Furthermore, continuous monitoring and regular impact assessments appear crucial for mitigating the negative effects of ARSs, as some problems may only become apparent in use.[1563] Nevertheless, the continuous monitoring tasks are

1556 (Skitka et al. 2000).
1557 (Huang et al. 2024, 2).
1558 If the LLM-based recruitment systems have been in use for a while and the human recruiters start to get the information and recommendations more granted, there is a risk that systems which initially have not involved ADM will do so without employers' awareness.
1559 Already when drafting the AIA, this issue was brought up by, among others, the EDPB and EDPS, see (EDPB and EDPS 2021, 12–13). Of prior research, see also (Tutt 2016).
1560 GDPR Art. 36. See sections 5.2.3 and 6.1.1.4 above.
1561 GDPR Art. 36.
1562 For instance, the Finnish Data Protection Ombdusman reported that it received in 2024 only 11 prior consultation cases (Finnish Data Protection Ombudsman 2024, 46) and the Swedish data protection authority received 12 prior consultations cases in the same year (Integritetsskydds myndigheten (IMY) 2025, 36). These numbers suggest that prior consultations are very rare, at least in the Nordics.
1563 See, e.g., AIA Recital 93.

currently set mainly for employers[1564] and providers[1565], and not for external auditors. Despite their powers to investigate ARSs, supervisory authorities can assess only a fraction of the systems in use, due to limited resources.[1566] Considering the employer's administrative burden and limited public resources, these limitations are understandable, but job applicants would benefit from the external evaluation of ARSs.

The limited external oversight mechanisms highlight the importance of employers' and providers' decisions regarding the design, development, and deployment of ARSs in securing the effectiveness of the safeguards.[1567] However, considering the above-discussed problems with preventive measures, those might not provide the required protection. Accordingly, ex-post enforcement, whether conducted by supervisory authorities or by job applicants, is important for ensuring that the safeguards are complied with and that potential rights infringements are remedied.

However, job applicants' enforcement efforts face practical and structural obstacles, creating the third shortcoming of the legal safeguards. Namely, detecting rights infringements within ARSs is hard, particularly for job applicants who have only limited information about the systems and lack access to them. After being rejected for a job opportunity, applicants may receive only an email stating that they were not chosen for the position. Where the decision has been automated or supported by a high-risk AI system, the job applicant may ask for an explanation of the decision. However, it remains unclear which specific information must be provided under the GDPR or the AIA, leaving room for divergent interpretations.[1568] Accordingly, employers decide what details about ARSs and explanations of their decision-making they provide, thereby determining what is revealed and what remains undisclosed.[1569] There is an inherent tension between employers' interests in drafting explanations, particularly in minimising legal or reputational risks, and job applicants' interests in understanding the evaluation criteria, detecting possible illegality, and obtaining evidence. This tension could influence the content of the explanations. Furthermore, the information provided to job applicants must be significantly simplified to ensure it is both understandable and practical for its

1564 AIA Art. 26(5) and GDPR Arts. 24 and 35.
1565 AIA Art. 72.
1566 Of the limited resources in GDPR enforcement, see, e.g., (European Union Agency for Fundamental Rights 2024).
1567 Although this dissertation focuses on the use phase of the ARS lifecycle, many of the safeguards should, however, be acknowledged throughout the system's lifecycle.
1568 See sections 6.1.2, 5.2.2 and 5.2.4 above.
1569 See also (Busuioc et al. 2023, 81–82).

intended purposes, that is, exercising data subject rights or contesting decisions[1570]. Yet finding the right balance between the specificity, understandability, and usefulness of the explanations is tricky.

Providing understandable and practical information about LLM-based recruitment systems, whose operations remain a mystery to employers and to some extent also to providers, is a considerable challenge.[1571] When providing the information and explanations required by the GDPR and AIA, employers must typically rely on provider-supplied details, with limited ability to verify their accuracy.[1572] For job applicants, verifying the accuracy of information and explanations regarding intractable LLM-based recruitment systems can be particularly difficult.[1573] However, similar problems also arose with the prior generation of ARSs and with fully human-conducted recruitment. For high-risk AI systems, job applicants could regularly access information about the systems from the EU database, which might help them verify that the disclosures align with the instructions for use and other documents.[1574] Nevertheless, the documentation available in the database is issued by the provider and is unlikely to contain any damning information.[1575]

The mediated and simplified nature of the information and explanations could undermine their effectiveness in detecting and contesting data protection breaches and discriminatory practices in ARSs. At the same time, full disclosure of the ARS's

[1570] AIA Recital 171 and C-203/22 *Dun & Bradstreet Austria*, paras 53-54. See also (Metikoš 2025).

[1571] According to public sources, LLM-based systems may defy full comprehension even by experts who have unmediated access to the system and its data, a thorough understanding of how these are constructed, and the freedom to test and experiment with the system (OECD 2023, 35; Bowman 2023, 6).

[1572] Research into the explainability of LLMs is bourgeoning, and ways to enhance human understanding of those could be further developed, see, e.g., (Goktas 2024, 22; Bhattacharjee et al. 2024; Wu et al. 2024; Cambria et al. 2024).

[1573] Self-explanations, where the LLMs are developed to explain their reasoning, for instance through chain-of-thought reasoning, articulating why or how they arrived at a given outcome, represent a potentially noteworthy development in this regard (Wu et al. 2024, 31–33; Bhattacharjee et al. 2024). Where providers and deployers are unable to tamper with such explanations, they could offer a new avenue for unmediated transparency. Since employers would have no ability to influence the explanations, they would have an incentive to review the explanations before acting on the outcomes. Where an explanation hints at potential illegality, the deployer would face a conscious choice of whether to proceed, bearing full legal responsibility for that decision.

[1574] For instance, the electronic instructions for use should be available through the EU database. See, e.g., AIA Art. 71(4) and Annex VIII Section A, point 12. Of the potential usefulness of the information contained in the EU database, see, e.g., (Publication IV / Parviainen 2026).

[1575] See also (Publication IV / Parviainen 2026).

code and documentation might not yield better results, given the system's intractability. For instance, proxies for protected grounds could remain undetectable to humans even if made visible.[1576] Supervisory authorities' ability to detect unlawful practices appears greater, as they are entitled to access more information than job applicants and can test systems.[1577]

Yet even where rights infringements are detected and pursued through judicial proceedings, proving them in court presents considerable challenges. As discussed in prior scholarship, including Publication III, obtaining evidence from opaque ARSs is difficult, if not impossible.[1578] Despite the alleviated burden of proof in non-discrimination cases and, to some extent, in data protection cases,[1579] job applicants are still required to present facts and evidence to establish their claims. With limited access to the systems and the simplified information and explanations provided by employers, establishing facts sufficient to support claims of data protection or non-discrimination violations could prove prohibitively demanding.[1580] The potentially short time limits for bringing a case also make it more difficult to gather the required evidence within that timeframe.[1581] However, as will be discussed in the following subchapter, there are interpretative avenues for addressing some of these challenges.

There are certain practical obstacles related to legal proceedings that may nevertheless reduce job applicants' willingness and ability to bring legal claims. When many of the legal parameters that safeguard job applicants are vaguely worded and leave room for interpretation, at least until case law fills the gaps, the outcomes of enforcement procedures remain highly uncertain.[1582] Furthermore, legal procedures require considerable legal and technical knowledge, time and money, which are not at every job applicant's disposal. As the outcomes remain highly

1576 See, e.g., (Prince and Schwarcz 2020, 1304; Wachter 2022, 158–59; Publication III / Parviainen 2024, 443).

1577 See GDPR Art. 58, AIA Art. 74 and Market Surveillance Regulation Art. 14. See also (Publication IV / Parviainen 2026).

1578 (Publication III / Parviainen 2024; Gerards and Xenidis 2020, 74–75; Hacker 2018, 1168; Wachter et al. 2021, 6).

1579 See, e.g., (Van Alsenoy 2016, 283) and section 6.1.3.2 above.

1580 Yet, some evidence of biases could possibly be derived with extensive testing by job applicants without access to the systems, see, e.g., (Yin et al. 2024).

1581 See also (Chopin and Germaine 2023, 86). In Finland, for instance, a claim for compensation concerning discrimination in recruitment must be made within a year from when the discriminated applicant received notice of the selection decision, see Section 26 of the Non-Discrimination Act (1325/2014).

1582 *Isabelle Choping and Catharina Germaine* have also found in their comparative analysis of non-discrimination law that the complexity of discrimination law may be an inhibiting factor (Chopin and Germaine 2023, 85).

uncertain and the complexity of the cases could increase legal costs, the cost risk is also an inhibiting factor. [1583]

Finally, the available remedies constitute the fourth shortcoming of the legal safeguards. Namely, even where job applicants after burdensome legal proceedings succeed in proving that their rights to data protection or non-discrimination have been infringed, the best remedy they can receive is compensation for the damage caused, not a job. Considering the difficulties job applicants face in legal proceedings, this equation likely does not appear tempting to many. Thus, the effectiveness of the safeguards should not rely on job applicants' shoulders.[1584]

Nevertheless, taken together, the above-discussed shortcomings appear to lead to an overemphasis on job applicants' private enforcement of the legal safeguards.[1585] The shortcomings with the preventive measures and limited external oversight emphasise the job applicants' role in enforcing their rights.[1586] Simultaneously, the problems of detecting infringements and proving them in court highlight the weaknesses of this approach, which burdens job applicants and does not provide robust protection.

The following subchapter explores the interpretative avenues available to address these shortcomings, even without legislative reforms.

6.3 Strengthening the existing safeguards

In addition to the shortcomings, this dissertation has also examined several ways to strengthen the existing legal safeguards. Given the primarily legal dogmatic approach, the solutions are mainly interpretative, and legislative reforms have mostly been left out of the scope.[1587]

Since many legal safeguards entail considerable interpretative leeway, their strength ultimately depends on how courts interpret them. Considering the aims of

1583 See also (Chopin and Germaine 2023, 85–86).
1584 See also (Shavell 1993, 267–69).
1585 Of private enforcement, see, e.g., (Shavell 1993, 266–67; Lafarre 2023, 232).
1586 Private enforcement by individuals is a typical model of enforcing EU law. While enabling individuals to exercise their rights under EU law, the doctrine of direct effect can also be seen as making individuals the primary supervisors of the EU legal order. See, e.g., (Weilert 1991, 2414; de Witte 2011, 359). Already in case-26/62 *van Gend en Loos*, p. 13, the vigilance of individuals to protect their rights was deemed important, although, additional to the supervison of the Commission and Member States.
1587 See section 1.4.1 above. Publication IV is an exception in this regard, as it contains also a few suggestions for legislative change, see (Publication IV / Parviainen 2026).

the GDPR[1588] and the Non-Discrimination Directives,[1589] as well as the AIA[1590] in many places, a teleological interpretation could lead to the strengthening of the legal safeguards and protection for job applicants' fundamental rights to data protection and non-discrimination, as well as to an effective remedy.[1591] However, such interpretations must also respect the employers' freedom to conduct a business, among other interests.[1592] Thus, balancing of competing rights and interests is required.

This dissertation has found that the strength of several preventive safeguards, including the applicability of the bans, might be reinforced through interpretation. For instance, a literal reading of AIA Article 5(1)(c) would ban all evaluation practices that fulfil the criteria of social scoring, covering, among other practices, the use of credit scoring in employment decision-making, and would not allow evaluation practices under national law.[1593]

In many places, a teleological reading could lead to broader protections, as the CJEU's prior case law indicates. The GDPR Article 22 ban on ADM has already been interpreted teleologically by the CJEU in a manner that could also protect job applicants' rights. Specifically, the CJEU has confirmed that the 'right not to be subject to a decision based solely on automated processing' constitutes a prohibition.[1594] Further, the CJEU has held that the decisions are to be interpreted broadly, and in a way which 'reinforces the effective protection intended by that provision'.[1595] In the *Schufa* case, automated decision-making was deemed to take place when a credit agency provided a probability value on which a third party drew strongly[1596] to establish, implement, or terminate contractual relationships.[1597] A similar protective reading could be extended to recruitment decision-making, where humans are only nominally involved. Such an interpretation could ensure that the ban on ADM also applies in the recruitment context, where human involvement remains important, especially at later stages of the recruitment process.

Teleological interpretation also holds promise in the context of non-discrimination legislation. For instance, based on the CJEU's prior case law, it may

1588 See GDPR Art. 1 and Recitals 1 and 10. See also section 1.3.3.
1589 RED Art. 1, EED Art. 1 and GED Art. 1. See also section 1.3.3.
1590 AIA Art. 1. See also section 1.3.3.
1591 CFREU Arts. 8, 20-21 and 47. Of the teleological interpretation, see section 1.4.2.
1592 CFREU Art. 16. See also CFREU Art. 17.
1593 For a more detailed discussion, see section 5.2.1.1 above.
1594 C-634/21 *Schufa*, para 52.
1595 C-634/21 *Schufa*, para 60. The CJEU has emphasised the individual rights protective purpose of the GDPR Art. 22, see para 57.
1596 In the *Schufa* case, 'in almost all cases' an insufficient probability value led to refusing a loan. C-634/21 *Schufa*, para 48.
1597 C-634/21 *Schufa*, para 73.

be possible to interpret the ban on direct discrimination as extending to proxy discrimination, as was proposed in Publication III.[1598] As long as the proxy is detectable and comprehensible to humans, the direct discrimination ban could pose a noteworthy constraint. However, to the extent that proxies are undetectable or incomprehensible, the reach of the ban on direct discrimination may weaken, unless the CJEU's doctrine of 'determining reasons'[1599] is broadened to also cover situations where the protected grounds have been included in the training data and thereby affected the decision.[1600] Yet, such an interpretation poses several practical difficulties and is unlikely to be adopted.[1601] Consequently, some proxy discrimination in ARSs likely falls outside the scope of the ban on direct discrimination.

Nevertheless, the ban on indirect discrimination could also be strengthened through interpretation in the algorithmic recruitment context. As the indirect discrimination ban allows justification of provisions, criteria, or practices that lead to particular disadvantages, the way the justifications are interpreted in the algorithmic discrimination context could significantly affect the protection the ban provides.[1602] Under a teleological interpretation of legitimate aims, for instance, aims that perpetuate existing biases and do not advance substantive equality could be deemed illegitimate.[1603] Further, instead of assessing system-level appropriateness, courts could evaluate the appropriateness criteria at the level of the features used by ARSs, making it practically impossible to justify an intractable ARS.[1604] Such a stricter interpretation of the justification possibilities could strengthen the reach of the ban on indirect discrimination.

1598 See (Publication III / Parviainen 2024, 443–48). See also sections 4.3 and 5.2.1.2 above.
1599 See C-83/14 *Chez,* paras 76-77. Of the reasoning-oriented approach, see also (Campbell and Smith 2020; 2023).
1600 See (Publication III / Parviainen 2024, 448–50).
1601 Although it might combat discrimination and put into effect the principle of equal treatment as the Non-Discrimination Directives aim (see RED Art. 1, EED Art. 1 and GED Art. 1), it could increase the employer's risk of using algorithmic systems considerably, possibly also constraining the freedom to conduct business. Furthermore, research has shown that processing of protected grounds may also be needed in the development phase to ensure that biases are detected and corrected (Žliobaitė and Custers 2016). This need for processing protected grounds is also reflected in the AIA Art. 10(5).
1602 See section 5.2.1.2 above.
1603 See also (Kelly-Lyth 2023, 156).
1604 See also (Kelly-Lyth 2023, 156; Hacker 2018, 1161; Grimmelmann and Westreich 2017, 173–74).

Beyond the Non-Discrimination Directives, job applicants might also be able to rely directly on CFREU Article 21[1605] where the situation falls within the scope of EU law.[1606] In Publication III, I argued that this could be the case, for instance, where the GDPR or AIA applies to the ARS.[1607] Invoking the CFREU's non-discrimination provisions could bring additional protected characteristics within the scope of protection.[1608] Accordingly, it could protect job applicants in a wider range of discrimination situations, as the criteria ARSs rely on could be varied.

A teleological interpretation of the principles of processing personal data could similarly reinforce the preventive safeguards. For instance, if the principle of accuracy were applied strictly in a manner that protects job applicants, it could prevent the use of LLM-based recruitment systems that are prone to confabulations, which cannot currently be entirely eliminated. Especially in the recruitment context, where decisions based on inaccurate data could deprive a job applicant of a job opportunity, such a strict interpretation may be necessary. The right to rectification and the right to effective remedies, which may be used in case of processing inaccurate personal data, do not, however, guarantee the applicant a job.[1609]

Taken together, if adopted by courts and authorities, these interpretations could lead diligent employers to avoid at least certain types of ARSs, such as LLM-based recruitment systems, if accuracy cannot be guaranteed before decision-making. Yet, the suggested interpretations would not prevent employers from utilising any ARSs whatsoever. Rather, these interpretations could target only the most problematic systems that involve, for instance, unacceptable risks in AI systems, automated decision-making or discrimination. In the absence of ex-ante external oversight and with a modest risk of enforcement, the preventive safeguards could, nonetheless, still have limited effects. However, there are also avenues to increase the likelihood of successful enforcement.

Turning to informational and remedial safeguards, the rights to explanations could be read in the light of their purpose: to provide job applicants with the

1605 In some situations, also CFREU Art. 20 or 23 could come into question. See also (Publication III / Parviainen 2024, 452–53).

1606 CFREU Art. 51(1). See also Case C-617/10 *Åkerberg Fransson*, paras 19–23 and 28; and C-206/13 *Siragusa*, paras 25–30.

1607 (Publication III / Parviainen 2024, 454).

1608 Of the protection provided by the CFREU's prohibition of discrimination, see also (Publication III / Parviainen 2024, 452–55).

1609 However, views arguing for disregard of GDPR's principle of processing have also been presented. For instance, *Etienne Drouard et al.* have deemed that some of the GDPR's requirements are impossible for AI systems to meet and should thus be excluded. See (Drouard et al. 2024b, 304). Yet, the EDPB clearly deems that 'technical impossibility cannot be invoked to justify non-compliance' with the GDPR's requirements (EDPB 2024c, 5).

information they need to exercise their rights and contest decisions made by or with the help of ARSs. Although the type of evidence required to bring a case varies in each instance, the details should be determined in the light of this aim of the explanations.[1610] If the characteristics of the ARS impede the provision of sufficient explanations, the employer may be considered responsible for demonstrating compliance with the key legal parameters. Otherwise, resorting to remedies could be practically impossible or excessively difficult for job applicants, thereby breaching their right to effective remedies granted under CFREU Article 47. Accordingly, an alleviation of the job applicants' burden of proof is necessary, not only in cases of alleged discrimination, where the Non-Discrimination Directives also contain an explicit alleviation of the burden of proof, but also in cases of breaches of the GDPR. As the procedural questions are left for the Member States' discretion, additional alleviations of the burden of proof may also be provided for in national legislation. If the legislation does not provide practical means to resort to remedies, job applicants may also directly invoke CFREU Article 47, which has horizontal direct effect.[1611]

As regards enforcement more broadly, prior research has argued that public enforcement should be the primary avenue where violations are complex and hidden.[1612] These are precisely the characteristics of data protection breaches and discrimination risks inherent in ARSs. Accordingly, rather than burdening job applicants with enforcement, supervisory authorities should play a prominent role in enforcing the legal safeguards and ensuring that the preventive safeguards are properly implemented.[1613] As supervisory authorities have the greatest capacity to enforce preventive safeguards, both in terms of access to information and expertise to investigate systems, they should also be granted adequate resources to conduct their tasks.[1614] Their investigations might reveal more systemic problems within ARSs and help address them more broadly across the labour market. However, authorities will likely target their investigations either to especially high-risk systems or to systems that have been complained about or reported.

The role of job applicants and the organisations representing them in triggering the supervisory authorities' investigations could therefore be considerable. Increasing job applicants' knowledge of their rights and enforcement options could increase the likelihood of supervisory investigations and legal proceedings, thereby

1610 Regarding the AIA's explanation, see AIA Recital 171, and regarding the GDPR, see C-203/22 *Dun & Bradstreet Austria*, para 55.
1611 See, e.g., C-414/16 *Egenberger,* para 78.
1612 (Shavell 1993, 267; Lafarre 2023, 232).
1613 Of the enforcement challenges data protection authorities face, see, e.g., (Abraha 2023, 186; European Union Agency for Fundamental Rights 2024).
1614 See also (Publication IV / Parviainen 2026).

creating pressure for employers to take the safeguards seriously. Organisations representing job applicants, whether non-profit organisations or trade unions[1615], potentially have greater technical and financial resources to investigate systemic problems in ARSs. These organisations could collectively use the rights of job applicants under the GDPR and the AIA to request details on how the ARS processed their applications.[1616] Aggregating such information might reveal, for instance, that a particular group of job applicants has been systematically disadvantaged by an ARS, potentially giving rise to complaints or claims.[1617]

The mainly interpretative solutions discussed in this section could be the starting point for enhancing the existing safeguards. While these solutions could provide job applicants with stronger protection under EU legislation, they could also impose stricter constraints on the use of certain ARSs.

[1615] In some cases, workers might see job applicants as their competitors, causing potential conflicts of interest for workers' representatives if they had to represent both current and potential workers. On the lack of interest of trade unions in representing and advocating for job applicants in the targeted online advertising scenario, see also (Parodi 2024, 120).

[1616] Job applicants can, of course, share information online without any intermediaries, but investigating and advocating for their cause requires considerable resources, which job applicants might lack.

[1617] The increased access to documentation proposed in Publication IV could also facilitate collective inquiries and contestation of high-risk AI recruitment systems. However, currently, access to the documentation reqauired by the AIA is limited mainly to the relevant national competent authorities or authorities protecting fundamental rights, which are subject to confidentiality obligations. See AIA Arts. 11–13, 17–19 and 74(12).

7 Conclusions

When this project commenced, the use of AI and other algorithmic systems in recruitment was expanding. However, the understanding of how EU legislation constrains the use of such ARSs and protects job applicants against the risks these systems pose remained limited. Accordingly, in this dissertation, I set out to provide a comprehensive and systematised account of how EU legislation constrains and shapes employers' use of ARSs and to examine the existing EU-level safeguards for job applicants, considering also their adequacy. Over the course of the project, both technical advancements in AI and significant legislative developments have further underscored the importance of these questions. In addressing them, this dissertation makes three principal scholarly contributions: a systematised framework of key legal parameters for ARS use, an integrated analysis of job applicants' legal safeguards across multiple EU legal instruments, and an evaluative assessment of their adequacy.

To pursue the aims of this dissertation, I adopted mainly a problem-based legal dogmatic approach with a systematising component, interpreting and systematising relevant provisions across multiple EU legislative instruments. Since the analysis centres on the use of ARSs that involve AI or algorithmic decision-making, it was necessary first to define these concepts and examine the ARSs' technological evolution. In particular, I traced how ARSs have developed from narrow, task-specific systems to LLM-based recruitment systems and beyond, and mapped their key technical characteristics, which also affect the legal analysis.

The first research question, how EU legislation constrains and shapes employers' use of ARSs that involve AI or algorithmic decision-making, was addressed through the framework of key legal parameters for ARS use. The framework divides the legal parameters into bans, obligations, specific duties, and actionable rights, and the ARSs into different system types that trigger varying legal parameters. The framework demonstrates that ARS use is subject to a plethora of legal parameters that vary, among other factors, in scope, normative target, strictness, and enforceability. By systematising the EU's fragmented legal landscape, the framework provides stakeholders, such as employers, job applicants, and authorities, with an analytical tool for navigating this constantly evolving regulatory

environment. It also provides the analytical foundation for addressing the second research question, as the legal parameters form the basis of the job applicants' legal safeguards. However, as the scope of the framework of key legal parameters is limited to the use phase, the EU level, and the risks related to data protection violations and discrimination, it may serve only as a starting point for legal analysis in specific cases.

The framework of key legal parameters shows that only a few ARS use cases, such as social scoring in AI-based systems, are categorically banned, while many ARSs remain permissible. However, the employer must ensure compliance with the relevant legal parameters applicable to the specific type of ARS throughout the use phase. Based on the framework, employers that use high-risk AI recruitment systems that make automated decisions carry the heaviest compliance burden, as those two system types together activate the most extensive set of legal parameters. Nevertheless, even these systems remain permissible provided the employer ensures full compliance with the applicable legal requirements.

Moreover, due to their broader scope and flexibility, other legal parameters may have a greater constraining and shaping effect on ARS use than absolute bans. However, these other legal parameters are also more vague, and the way those should be interpreted is not yet established. For instance, whenever using an ARS, employers must ensure that the ARS use does not breach the qualified bans on discrimination, processing of special category data or ADM. Furthermore, more general obligations and actionable rights stemming especially from data protection legislation, such as the principles governing the processing of personal data, could, in practice, constrain and shape most ARSs, limiting the means they could employ. For example, if interpreted strictly, the general obligations could severely limit the lawful use of LLM-based ARSs that tend to confabulate. The specific duties, together with the actionable rights, primarily shape the processes of how ARS should be used. The specific duties may, for instance, direct the way ARSs are monitored and how the humans operating the ARSs are trained, while actionable rights may affect how job applicants are informed of ARS's decisions. Actionable rights simultaneously function as legal entitlements that job applicants may directly invoke, linking the framework of key legal parameters to the safeguard analysis.

The framework of key legal parameters formed the basis for answering also the second research question: what legal safeguards EU legislation provides to protect job applicants against data protection infringements and discrimination arising from the use of ARSs that involve AI or algorithmic decision-making, and how adequate those safeguards are. However, the second research question was approached through a safeguards-based typology distinguishing between preventive, informational, and remedial safeguards.

Turning first to preventive safeguards, from the perspective of job applicants, many of the legal parameters function preventively. Nevertheless, the ambiguity of the legal parameters and characteristics of the ARSs, such as the complexity, uninterpretability, indeterminacy, and unpredictability of the LLM-based recruitment systems, could complicate employers' efforts to comply with the legal parameters, diminishing their preventive effects. In the algorithmic recruitment context, ex-ante oversight is limited to situations where employers consult data protection authorities following a DPIA. Consequently, employers have considerable discretion in implementing the preventive safeguards as they see fit, and non-compliance may often remain undetected.

For example, the exceptions inherent in qualified bans and the ambiguities in the principles of processing personal data could initially be interpreted by the employer as permitting ARS use. However, given the ambiguities in the legal parameters, the lack of case law on algorithmic systems, and the limited guidance from the authorities on the matter, the employer may struggle to ascertain that the solution they adopted is lawful. Should the employer's use of ARS be challenged in court, the court may adopt a more restrictive interpretation, leading to a finding of non-compliance. Such a finding could have significant consequences for the employer, including administrative fines or orders, damages payable to job applicants, or even criminal sanctions under national law, thereby enhancing the legislation's preventive effects. Yet, due to the weak ex-ante oversight mechanisms, the likelihood of enforcement actions could remain relatively modest. This is because job applicants face structural barriers to enforcement and lack incentives to initiate enforcement measures, thereby reducing the legislation's preventive effects.

The informational safeguards under the GDPR and the AIA could somewhat assist job applicants' enforcement measures by raising awareness of ARS use, facilitating detection of infringements, and enabling evidence to be obtained for claims against employers. However, the informational safeguards also have their limitations. Employers ultimately decide what information job applicants are provided, as the provisions contain rather vague wording and do not require providing access to the systems. Furthermore, the complexity of the systems makes it difficult for employers to explain their use in a manner that facilitates enforcement. These limitations significantly reduce the likelihood that the available information will reveal infringements or provide sufficient evidence to support claims.

Remedial safeguards offering job applicants a means of redress if infringements are detected and proven also exist in EU legislation. From the job applicants' perspective, the most potent remedies are the traditional judicial remedies, which may result in an award of compensation under the GDPR, national non-discrimination legislation, or national tort law. Nonetheless, the judicial remedies also require the most resources and evidence from applicants, making them

burdensome to utilise in practice. Even in discrimination claims, where the burden of proof should be explicitly alleviated by national legislation, job applicants still need to establish facts from which it can be presumed that discrimination has occurred. This is a challenging task given the increasing intractability of ARSs. Moreover, even where the job applicants' claims are successful, they may, at best, receive some monetary compensation, while the job opportunity is irreparably lost.

Supervisory authorities, however, have access to the ARSs and have better resources and capabilities to investigate the systems. Hence, filing complaints with supervisory authorities can help detect infringements, as their investigations may uncover breaches without requiring substantial resources or evidence from job applicants. The investigations might also provide some evidence to support job applicants' claims in court. Nevertheless, given the authorities' scarce resources, they may primarily investigate ARSs that have been reported or complained about, which again emphasises the need for job applicants' actions.

Drawing on these findings across both research questions, I argue that *despite the multiple constraints and conditions imposed on employers' use of ARSs, the EU-level legal framework remains inadequate to protect job applicants from the risks posed by ARSs that involve AI or algorithmic decision-making.* The EU-level legal framework presents a twofold problem. For employers, compliance is a profound challenge, as ARS use is subject to numerous legal parameters, many of which are vague or open-ended and include considerable sanctions for non-compliance. Even if the legal parameters were clear, ensuring compliance could be difficult as the ARSs are complex and opaque, and employers may struggle to sufficiently understand and affect their workings to adhere to the legal parameters. For job applicants, the legal safeguards under existing EU legislation often fall short, failing to adequately prevent infringements of their rights to data protection and non-discrimination or to provide effective remedies once violations occur. This inadequacy stems primarily from four distinct but related factors: the vagueness of the legal parameters governing ARS use, the limited ex-ante oversight mechanisms, the structural barriers to enforcement by job applicants, and the inherent limitations of the available remedies.

As mentioned above, the legal parameters absolutely prohibit only a few specific ARS use cases, while most ARS use remains permissible but is subject to multiple vague legal parameters, particularly concerning data protection, non-discrimination, and transparency. The vaguely formulated legal parameters, together with the intractability of ARSs, complicate compliance. Since there is no systematic ex-ante oversight of ARSs, the role of ex-post enforcement in securing job applicants' rights to data protection and non-discrimination is emphasised. If supervisory authorities do not have sufficient resources to investigate ARSs and enforce the legislation, the primary responsibility for detecting faults and breaches and making employers

accountable for those falls on job applicants and the organisations representing them. Yet, the ex-post enforcement faces several structural obstacles. The vague legal parameters make it more difficult for job applicants to analyse whether those are breached or not. Further, job applicants have limited access to unmediated information about the ARSs. Accordingly, they often lack the information needed to detect rights violations. Even when rights violations are suspected, proving such allegations in judicial proceedings poses a further challenge. The modest probability of successful enforcement also weakens the deterrent effect of the legal parameters in practice, reducing employers' incentive to ensure compliance and leaving job applicants with limited assurance that the legal parameters will be observed.

Encouragingly, there are avenues for improvement even within the existing legal framework. If the courts decide to adopt teleological and fundamental rights-protective interpretations of the legal parameters, the constraining effects of EU legislation could be more robust and protective of job applicants than the initial analysis suggests. For instance, as regards the justifiability of indirect discrimination or the effects of the principles of processing personal data, a teleological interpretation of the key legal parameters could lead to stronger constraints on ARSs. Moreover, the CFREU Article 47 right to an effective remedy could be interpreted to shift the burden of proof at a lower evidentiary threshold to the employer using the ARSs, for example, in cases where the intractability of the ARS makes it excessively difficult for job applicants to provide evidence of rights-infringing ARS use. This interpretation would render the use of inexplicable ARSs excessively risky for most employers, thereby significantly curtailing their deployment. However, while such an interpretation could help prevent the spreading of certain risky ARSs, it might simultaneously restrict systems that could help mitigate and correct human recruiters' biases in decision-making. Furthermore, these interpretative solutions help only if applicants can initiate proceedings in the first place and do not resolve the limitations of the available remedies.

Beyond interpretative solutions, targeted legislative changes to address specific shortcomings in the current text of the AIA were proposed in Publication IV, including, for instance, an obligation to inform job applicants of the existence of the EU database for high-risk AI systems when a high-risk AI system is used in the recruitment process. However, more profound legislative changes could be needed to ensure the adequate protection of job applicants' fundamental rights in algorithmic recruitment. Yet, as Publication IV demonstrated, it is not only EU-level legislation that may address the shortcomings; also, standards, authorities' guidance, national legislation, collective agreements and informational campaigns could be used to patch some of the deficiencies.

Given the constant flux in both technological and legal landscapes, there is much to explore in future research. Future studies could build on the interpretative insights

and targeted de lege ferenda proposals to explore more comprehensive legislative reforms. The framework of key legal parameters proposed in this dissertation could be applied in future studies examining, for instance, the effects of upcoming EU legislative initiatives or emerging agentic AI systems on job applicants. With certain adaptations, it could also support analyses of employees' legal protection when AI and algorithmic decision-making are used at the workplace. Furthermore, empirical studies are needed to investigate how legal safeguards are enforced in practice, as such investigations might reveal shortcomings not addressed in this legal-dogmatic study. Finally, interdisciplinary research that combines legal, technical, and human resources perspectives is essential to ensure that, if ARSs are adopted, they comply with the legislation, are technically sound, meet employers' needs, and enhance job applicants' fundamental rights.

Until future case law and research clarify the situation further, this dissertation should assist employers in meeting their compliance obligations and minimising risks to job applicants' rights. At the same time, job applicants and their representatives can use the proposed framework and analysis to inform their enforcement efforts. Although job applicants' enforcement actions may not result in securing the job in question, they can expose deeper systemic issues within ARSs, ultimately contributing to fairer and more transparent recruitment practices.

Abbreviations

ADM	automated decision-making
AG	Advocate General
AI	artificial intelligence
AIA	Artificial Intelligence Act
ARS	algorithmic recruitment system
API	application programming interface
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
COE	Council of Europe
CSDDD	Corporate Sustainability Due Diligence Directive
DPA	data protection authority
DPIA	data protection impact assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EED	Employment Equality Directive
EU	European Union
FAD	Framework Agreement on Digitalisation
FRIA	fundamental rights impact assessment
GDPR	The General Data Protection Regulation
GED	Gender Equality Directive
GPAI	general-purpose AI
GPT	generative pre-trained transformer
HR	human resources
ILO	International Labour Organization
IPR	intellectual property rights
LLM	large language model
ML	machine learning
MS	Member State
NLP	natural language processing
OECD	Organisation for Economic Co-operation and Development

PLD	Product Liability Directive
PTD	Pay Transparency Directive
PWD	Platform Work Directive
RAG	retrieval augmented generation
RED	Race Equality Directive
SME	small and medium-sized enterprise
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
WP29	Article 29 Working Party

List of References

Aarnio, Aulis. 1978. *Mitä lainoppi on?* Forum-oikeustiede. Kustannusosakeyhtiö Tammi. Helsinki.

Aarnio, Aulis. 1982. *Oikeussäännösten tulkinnasta: Tutkimus lainopillisen perustelun rationaalisuudesta ja hyväksyttävyydestä*. Juridica. Helsinki.

Aarnio, Aulis. 1989. *Laintulkinnan teoria*. Werner Söderström Osakeyhtiö. Juva.

Aarnio, Aulis. 2011. *Luentoja lainopillisen tutkimuksen teoriasta*. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Unigrafia Oy Yliopistopaino.

Abraha, Halefom. 2023. "Regulating Algorithmic Employment Decisions through Data Protection Law." *European Labour Law Journal* 14 (2): 172–91. https://doi.org/10.1177/20319525231167317.

Abraham, Vineet. 2025. "How Agentic AI Is Shaping the Future of Recruiting." *Eightfold*, March 10. <https://eightfold.ai/blog/li-agentic-ai-shaping-future-recruiting/>. (accessed 24.6.2025)

Ackerman, Lee. 2025. "Perceptions of Agentic AI in Organizations: Implications for Responsible AI and ROI." arXiv:2504.11564. Preprint, arXiv, April 15. https://doi.org/10.48550/arXiv.2504.11564.

Adams-Prassl, Jeremias. 2020. "Article 47 CFR and the Effective Enforcement of EU Labour Law: Teeth for Paper Tigers?" *European Labour Law Journal* 11 (4): 391–402. https://doi.org/10.1177/2031952520905383.

Adams-Prassl, Jeremias, Halefom Abraha, Aislinn Kelly-Lyth, Michael 'Six' Silberman, and Sangh Rakshita. 2023. "Regulating Algorithmic Management: A Blueprint." *European Labour Law Journal*, ahead of print, April 20. https://doi.org/10.1177/20319525231167299.

Adams-Prassl, Jeremias, Reuben Binns, and Aislinn Kelly-Lyth. 2023. "Directly Discriminatory Algorithms." *The Modern Law Review* 86 (1): 144–75. https://doi.org/10.1111/1468-2230.12759.

Agarwal, Deepak. 2018. "An Introduction to AI at LinkedIn." Linkedin. *LinkedIn Engineering Blog*, September 10. <https://www.linkedin.com/blog/engineering/ai/an-introduction-to-ai-at-linkedin>.

Agencia Española Protección Datos. 2019. "Indicative List of the Types of Data Processing That Do Not Require a Data Protection Impact Assessment Under Art. 35.5 GDPR."

AIAAIC. 2025. "AIAAIC Repository." AIAAIC. <AIAAIC.org>. (accessed 21.4.2025)

Ajunwa, Ifeoma. 2020. "The Paradox of Automation as Anti-Bias Intervention." *Cardozo Law Review* 41 (5): 1671–742.

Ajunwa, Ifeoma. 2023. *The Quantified Worker - Law and Technology in the Modern Workplace*. Cambridge University Press.

Alba, Davey, and Leon Yin. 2024. "Companies Should Think Twice Before Using Generative AI in Hiring." *Bloomberg Newsletter*, August 3. <https://www.bloomberg.com/news/newsletters/2024-03-08/companies-should-think-twice-before-using-generative-ai-in-hiring>. (accessed 21.11.2024)

Albert, Edward Tristram. 2019. “AI in Talent Acquisition: A Review of AI-Applications Used in Recruitment and Selection.” *Strategic HR Review* 18 (5): 215–21. https://doi.org/10.1108/SHR-04-2019-0024.

Albin, Einat. 2025. “The Three-Tier Structural Legal Deficit Undermining the Protection of Employees’ Personal Data in the Workplace.” *Oxford Journal of Legal Studies* 45 (1): 81–107. https://doi.org/10.1093/ojls/gqae033.

Alexander III, Leo, Q. Chelsea Song, Louis Hickman, and Hyun Joo Shin. 2025. “Sourcing Algorithms: Rethinking Fairness in Hiring in the Era of Algorithmic Recruitment.” *International Journal of Selection and Assessment* 33 (1): e12499. https://doi.org/10.1111/ijsa.12499.

Alexy, Robert. 2002. *A Theory of Constitutional Rights*. Translated by Julian Rivers. Oxford University Press.

Almada, Marco. 2019. “Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems.” *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law*, June 17, 2–11. https://doi.org/10.1145/3322640.3326699.

Almada, Marco. 2022. “A Frontier Talk: Foundation Models in AI: What Impact for Policies and Law? Speaker: Matthias Gallé (Naver Labs Europe).” ETUI.

Almada, Marco, and Nicolas Petit. 2023. “The EU AI Act: A Medley of Product Safety and Fundamental Rights?” *European University Institute Robert Schuman Centre for Advanced Studies Working Paper Series*.

Aloisi, Antonio. 2024. “Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights.” *International Journal of Comparative Labour Law and Industrial Relations* 40 (1): 37–70.

Alpaydin, Ethem. 2020. *Introduction to Machine Learning*. 4th ed. Adaptive Computation and Machine Learning Series. The MIT Press.

Amershi, Saleema, Andrew Begel, Christian Bird, et al. 2019. “Software Engineering for Machine Learning: A Case Study.” *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, May, 291–300. https://doi.org/10.1109/ICSE-SEIP.2019.00042.

Andrews, Caitlin. 2025. “Agentic AI’s Risk and Reward Calculus.” *IAPP*, April 16. <https://iapp.org/news/a/agentic-ai-s-risk-and-reward-calculus>. (accessed 24.6.2025)

ANP. 2025. “Job Adverts on Facebook Discriminate by Gender, Says Dutch Human Rights Institute | NL Times.” *NL Times*, February 18. <https://nltimes.nl/2025/02/18/job-adverts-facebook-discriminate-gender-says-dutch-human-rights-institute>. (accessed 26.3.2025)

Anthropic PBC. 2026. “Claude.” Claude. <https://claude.ai/login>. (accessed 20.2.2026)

Arnull, Anthony. 2006. *The European Union and Its Court of Justice*. Oxford EC Law Library. Oxford University Press.

Arthur, Winfred, Dennis Doverspike, Ted B. Kinney, and Matthew O’Connell. 2017. “The Impact of Emerging Technologies on Selection Models and Research.” In *Handbook of Employee Selection*, 2nd ed., edited by James L. Farr, Nancy T. Tippins, Walter C. Borman, et al. Routledge. https://doi.org/10.4324/9781315690193-44.

Arctic Shores. 2025. “Arctic Shores: Task-Based Assessments for Recruitment.” <https://www.arcticshores.com>. (accessed 26.3.2025)

Ausloos, Jef, and Pierre Dewitte. 2018. “Shattering One-Way Mirrors – Data Subject Access Rights in Practice.” *International Data Privacy Law* 8 (1): 4–28. https://doi.org/10.1093/idpl/ipy001.

Auxier, Brooke, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. *Americans and Privacy in 2019 - Concerned, Confused and Feeling Lack of Control Over Their Personal Information _ Pew Research Center*. Pew Research Center.

<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

AWS. 2024. “What Is RAG? - Retrieval-Augmented Generation AI Explained - AWS.” Amazon Web Services, Inc., September 12. <https://aws.amazon.com/what-is/retrieval-augmented-generation/>. (accessed 9.12.2024)

Aza, Asymina. 2024. “Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context.” *Industrial Law Journal*, August 29, 1–19. https://doi.org/10.1093/indlaw/dwae035.

Bai, Yuntao, Andy Jones, Kamal Ndousse, et al. 2022. “Training a Helpful and Harmless Assistant with Reinforcement Learning from Human Feedback.” arXiv:2204.05862. Preprint, arXiv, April 12. <http://arxiv.org/abs/2204.05862>.

Baldini, Davide, and Matteo De Benedetto. 2025. “The Open Texture of ‘Algorithm’ in Legal Language.” *AI & SOCIETY* 40 (3): 1643–54. https://doi.org/10.1007/s00146-024-01925-z.

Ball, Kirstie. 2010. “Workplace Surveillance: An Overview.” *Labor History* 51 (1): 87–106. https://doi.org/10.1080/00236561003654776.

Bamberger, Peter A., and Valeria Alterman. 2024. “Navigating the Practical Complexities of Pay Transparency: Implications for Employers and Public Policy.” *Compensation & Benefits Review* 56 (1): 37–48. https://doi.org/10.1177/08863687231189590.

Banerjee, Sourav, Ayushi Agarwal, and Saloni Singla. 2024. “LLMs Will Always Hallucinate, and We Need to Live With This.” arXiv:2409.05746. Preprint, arXiv, September 9. https://doi.org/10.48550/arXiv.2409.05746.

Barber, Alison E. 1998. *Recruiting Employees: Individual and Organizational Perspectives*. Thousand Oaks, Calif. London.

Barberá, Isabel. 2025. “AI Privacy Risks & Mitigations Large Language Models (LLMs).” EDPB.

Barnard, Catherine. 2012. *EU Employment Law*. 4th ed. Oxford University Press.

Barnard, Catherine. 2023. “The Serious Business of Having Fun: EU Legal Protection for Those Working Online in the Digital Economy.” *International Journal of Comparative Labour Law and Industrial Relations* 39 (2).

Barnard, Catherine, and Bob Hepple. 2000. “Substantive Equality.” *The Cambridge Law Journal* 59 (3): 562–85. https://doi.org/10.1017/S0008197300000246.

Barocas, Solon, and Andrew D. Selbst. 2016. “Big Data’s Disparate Impact.” *California Law Review* 104: 671–732. https://doi.org/http://dx.doi.org/10.15779/Z38BG31.

Barocas, Solon, Andrew D. Selbst, and Manish Raghavan. 2020. “The Hidden Assumptions Behind Counterfactual Explanations and Principal Reasons.” *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, January 27, 80–89. https://doi.org/10.1145/3351095.3372830.

Barrett, Lisa Feldman, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez, and Seth D. Pollak. 2019. “Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements.” *Psychological Science in the Public Interest* 20 (1): 1–68. https://doi.org/10.1177/1529100619832930.

Barros Vale, Sebastião, and Gabriela Zanfir-Fortuna. 2022. *FPF Report: Automated Decision-Making Under the GDPR - A Comprehensive Case-Law Analysis - Future of Privacy Forum*. Future of Privacy Forum. <https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/>.

Beck, Gunnar. 2013. *Legal Reasoning of the Court of Justice of the EU*. Bloomsbury Publishing.

Bekkum, Marvin van, and Frederik Zuiderveen Borgesius. 2022. "Using Sensitive Data to Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception?" *Computer Law & Security Review* 48: 105770. https://doi.org/10.1016/j.clsr.2022.105770.

Belanger, Ashley. 2023. "OpenAI Faces Defamation Suit after ChatGPT Completely Fabricated Another Lawsuit." Ars Technica, June 9. <https://arstechnica.com/tech-policy/2023/06/openai-sued-for-defamation-after-chatgpt-fabricated-yet-another-lawsuit/>. (accessed 17.12.2024)

Belavusau, Uladzislau, and Kristin Henrard. 2019. "A Bird's Eye View on EU Anti-Discrimination Law: The Impact of the 2000 Equality Directives." *German Law Journal* 20: 614–36.

Bengoetxea, Joxerramon. 1993. *The Legal Reasoning of the European Court of Justice - Towards a European Jurisprudence*. Clarendon Press Oxford.

Bercusson, Brian. 2009. *European Labour Law*. 2nd ed. Cambridge University Press. https://doi.org/10.1017/CBO9780511609831.

Bersin, Josh. 2023. *SeekOut Brings GPT4 To Recruiters. Eightfold Launches Copilots For HR.* April 4. <https://joshbersin.com/2023/04/seekout-brings-gpt4-to-recruiters-eightfold-launches-copilots-for-hr/>. (accessed 21.11.2024)

Bhattacharjee, Amrita, Raha Moraffah, Joshua Garland, and Huan Liu. 2024. "Towards LLM-Guided Causal Explainability for Black-Box Text Classifiers." arXiv:2309.13340. Preprint, arXiv, January 29. https://doi.org/10.48550/arXiv.2309.13340.

Bhattacharya, Aditya, and Katrien Verbert. 2025. "Let's Get You Hired: A Job Seeker's Perspective on Multi-Agent Recruitment Systems for Explaining Hiring Decisions." arXiv:2505.20312. Preprint, arXiv, May 22. https://doi.org/10.48550/arXiv.2505.20312.

Bick, Alexander, Adam Blandin, and David J Deming. 2024. *The Rapid Adoption of Generative AI*. Working Paper. National Bureau of Economic Research.

Binns, Reuben, and Michael Veale. 2021. "Is That Your Final Decision? Multi-Stage Profiling, Selective Effects, and Article 22 of the GDPR." *International Data Privacy Law* 11 (4): 319–32. https://doi.org/10.1093/idpl/ipab020.

Bird & Bird. 2024. "European Union Artificial Intelligence Act: Guide." June 11. <https://www.twobirds.com/-/media/new-website-content/pdfs/capabilities/artificial-intelligence/european-union-artificial-intelligence-act-guide.pdf>.

Black, J. Stewart, and Patrick van Esch. 2020. "AI-Enabled Recruiting: What Is It and How Should a Manager Use It?" *Business Horizons* 63 (2): 215–26. https://doi.org/10.1016/j.bushor.2019.12.001.

Bobek, Michal. 2014. "The Effects of EU Law in the National Legal Systems." In *European Union Law*, edited by Catherine Barnard and Steve Peers. Oxford University Press.

Bodie, Matthew T, Miriam A Cherry, Marcia L McCormick, and Jintong Tang. 2017. "The Law and Policy of People Analytics." *University of Colorado Law Review* 88: 961–1042.

Bogen, Miranda, and Aaron Rieke. 2018. *Help Wanted - An Examination of Hiring Algorithms, Equity, and Bias*. Upturn. <https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf>.

Bolander, Pernilla, and Jörgen Sandberg. 2013. "How Employee Selection Decisions Are Made in Practice." *Organization Studies* 34 (3): 285–311. https://doi.org/10.1177/0170840612464757.

Bommasani, Rishi, Drew A. Hudson, Ehsan Adeli, et al. 2021. "On the Opportunities and Risks of Foundation Models." *arXiv:2108.07258 [Cs]*, August 18. <http://arxiv.org/abs/2108.07258>.

Borgesius, Frederik J. Zuiderveen. 2020. “Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence.” *The International Journal of Human Rights* 24 (10): 1572–93. https://doi.org/10.1080/13642987.2020.1743976.

Bornstein, Stephanie. 2018. “Antidiscriminatory Algorithms.” *Alabama Law Review* 70 (2): 519–72.

Borrelli, Michael, Sean Musch, Doug Hohulin, et al. 2025. “Fostering Agentic AI: How the Development and Functionality of AI Agents – and the Implications of Their Use – Are Fostered by the EU AI Act, Particularly from a Risk Classification Standpoint, amid Rapid Advances in Large Language and Multimodal Models.” SSRN Scholarly Paper No. 5196814. Social Science Research Network, March 14. https://doi.org/10.2139/ssrn.5196814.

Bowman, Samuel R. 2023. “Eight Things to Know about Large Language Models.” arXiv:2304.00612. Version 1. Preprint, arXiv, April 2. https://doi.org/10.48550/arXiv.2304.00612.

Brameshuber, Elisabeth. 2021. “15. Information and Consultation Rights.” In *EU Collective Labour Law*, 1st ed., edited by Beryl ter Haar and Attila Kun. Edward Elgar Publishing Limited.

Brand, Dirk. 2020. “Algorithmic Decision-Making and the Law.” *JeDEM - eJournal of eDemocracy and Open Government* 12 (1): 114–31. https://doi.org/10.29379/jedem.v12i1.576.

Breaugh, James A. 2013. “Employee Recruitment.” *Annual Review of Psychology* 64 (1): 389–416. https://doi.org/10.1146/annurev-psych-113011-143757.

Breidbach, Christoph F. 2024. “Responsible Algorithmic Decision-Making.” *Organizational Dynamics* 53 (2): 101031. https://doi.org/10.1016/j.orgdyn.2024.101031.

Brkan, Maja. 2018. “The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to Its Core.” *European Constitutional Law Review* 14: 332–68.

Brkan, Maja. 2019a. “Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond.” *International Journal of Law and Information Technology* 27 (2): 91–121. https://doi.org/10.1093/ijlit/eay017.

Brkan, Maja. 2019b. “The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning.” *German Law Journal* 20 (6): 864–83. https://doi.org/10.1017/glj.2019.66.

Brkan, Maja, and Hana Palčič Vilfan. 2024. “Article 86 - Right to Explanation of Individual Decision-Making.” In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Broad, Ryan. 2024. *The Impact of Generative AI on Talent Acquisition in 2024*. Linkedin. February 10. <https://www.linkedin.com/pulse/impact-generative-ai-talent-acquisition-2024-ryan-broad-7oxje>. (accessed 24.6.2025)

Broecke, Stijn. 2023. *Artificial Intelligence and Labour Market Matching*. OECD Social, Employment and Migration Working Papers No. 284. Vol. 284. OECD Social, Employment and Migration Working Papers. OECD. https://doi.org/10.1787/2b440821-en.

Budhwar, Pawan, Soumyadeb Chowdhury, Geoffrey Wood, et al. 2023. “Human Resource Management in the Age of Generative Artificial Intelligence: Perspectives and Research Directions on ChatGPT.” *Human Resource Management Journal* 33 (3): 606–59. https://doi.org/10.1111/1748-8583.12524.

Buolamwini, Joy, and Timnit Gebru. 2018. “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.” Paper presented at Conference on Fairness, Accountability, and Transparency.

Búrca, Gráinne de. 2013. “After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?” *Maastricht Journal of European and Comparative Law* 20 (2): 168–84. https://doi.org/10.1177/1023263X1302000202.

Burrell, Jenna. 2016. “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms.” *Big Data & Society* 3 (1): 205395171562251. https://doi.org/10.1177/2053951715622512.

Bursell, Moa, and Lambros Roumbanis. 2024. “After the Algorithms: A Study of Meta-Algorithmic Judgments and Diversity in the Hiring Process at a Large Multisite Company.” *Big Data & Society* 11 (1): 20539517231221758. https://doi.org/10.1177/20539517231221758.

Busuioc, Madalina, Deirdre Curtin, and Marco Almada. 2023. “Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act.” *European Law Open* 2 (1): 79–105. https://doi.org/10.1017/elo.2022.47.

Buyl, Maarten, Christina Cociancig, Cristina Frattone, and Nele Roekens. 2022. “Tackling Algorithmic Disability Discrimination in the Hiring Process: An Ethical, Legal and Technical Analysis.” *2022 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA), FAccT ’22, June 20, 1071–82. https://doi.org/10.1145/3531146.3533169.

Bygrave, Lee A. 2002. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Information Law Series. Kluwer Law International.

Bygrave, Lee A. 2020. “Article 22. Automated Individual Decision-Making Including Profiling.” In *The EU General Data Protection Reuglation (GDPR): A Commentary*, edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Bygrave, Lee A., and Rebecca Schmidt. 2024. “Regulating Non-High-Risk AI Systems under the EU’s Artificial Intelligence Act, with Special Focus on the Role of Soft Law.” SSRN Scholarly Paper No. 4997886. Social Science Research Network, October 24. https://doi.org/10.2139/ssrn.4997886.

Calvi, Alessandra. 2023. “Exploring the Synergies between Non-Discrimination and Data Protection: What Role for EU Data Protection Law to Address Intersectional Discrimination?” *European Journal of Law and Technology* 14 (2).

Cambria, Erik, Lorenzo Malandri, Fabio Mercorio, Navid Nobani, and Andrea Seveso. 2024. “XAI Meets LLMs: A Survey of the Relation between Explainable AI and Large Language Models.” arXiv:2407.15248. Preprint, arXiv, July 21. https://doi.org/10.48550/arXiv.2407.15248.

Campbell, Colin, and Dale Smith. 2020. “The Grounding Requirement for Direct Discrimination.” *Law Quarterly Review* 136 (2): 258–83.

Campbell, Colin, and Dale Smith. 2023. “Distinguishing Between Direct and Indirect Discrimination.” *The Modern Law Review* 86 (2): 307–30. https://doi.org/10.1111/1468-2230.12760.

Cao, Yihan, Siyu Li, Yixin Liu, et al. 2023. “A Comprehensive Survey of AI-Generated Content (AIGC): A History of Generative AI from GAN to ChatGPT.” arXiv:2303.04226. Preprint, arXiv, March 7. https://doi.org/10.48550/arXiv.2303.04226.

Capasso, Marianna, Payal Arora, Deepshikha Sharma, and Celeste Tacconi. 2025. “On the Right to Work in the Age of Artificial Intelligence: Ethical Safeguards in Algorithmic Human Resource Management.” *Business and Human Rights Journal*, January 6, 1–15. https://doi.org/10.1017/bhj.2024.26.

Cappelli, Peter, Nikolai Rogovsky, and International Labour Organization. Research Department,. 2023. *Artificial Intelligence in Human Resource Management: A Challenge for the Human-Centred Agenda?* ILO. https://doi.org/10.54394/OHVV4382.

Carlini, Nicholas, Jamie Hayes, Milad Nasr, et al. 2023. “Extracting Training Data from Diffusion Models.” arXiv:2301.13188. Preprint, arXiv, January 30. https://doi.org/10.48550/arXiv.2301.13188.

Carter, Christine. 2024. “Why the Algorithmic Recruiter Discriminates: The Causal Challenges of Data-Driven Discrimination.” *Maastricht Journal of European and Comparative Law* 31 (3): 333–59. https://doi.org/10.1177/1023263X241248474.

Castellucia, Claude, and Daniel Le Métayer. 2019. *Understanding Algorithmic Decision-Making: Opportunities and Challenges.* Study PE 624.261. EPRS | European Parliamentary Research Service. <https://data.europa.eu/doi/10.2861/536131>.

Casu, Matteo. 2024. “Matching Skills and Candidates with Graph RAG.” Ontotext, May 31. <https://www.ontotext.com/blog/matching-skills-and-candidates-with-graph-rag/>.

Cecchetti, Lorenzo. 2024. “Unravelling Horizontal Direct Effect in EU Law: The Case of the Fundamental Right to Paid Annual Leave between ‘Myth’ and ‘Practice.’” *Yearbook of European Law* 42 (April): 42–83. https://doi.org/10.1093/yel/yead012.

Cefaliello, Aude, and Miriam Kullmann. 2022. “Offering False Security: How the Draft Artificial Intelligence Act Undermines Fundamental Workers Rights.” *European Labour Law Journal*, October 20, 203195252211144. https://doi.org/10.1177/20319525221114474.

Celeste, Edoardo, and Abhilash Nair. 2024. “2024: The Year of AI? Exploring the Role of Legal Scholarship and Interdisciplinary Research.” *European Journal of Law and Technology* 15 (2). <https://www.ejlt.org/index.php/ejlt/article/view/1020>.

Centre for Data Ethics and Innovation. 2021. *Review into Bias in Algorithmic Decision-Making*.

Chala, Sisay Adugna, Fazel Ansari, Madjid Fathi, and Kea Tijdens. 2018. “Semantic Matching of Job Seeker to Vacancy: A Bidirectional Approach.” *International Journal of Manpower* 39 (8): 1047–63. https://doi.org/10.1108/IJM-10-2018-0331.

Chalmers, Damian, Gareth Davies, Giorgio Monti, and Veerle Heyvaert. 2024. *European Union Law : Text and Materials*. Cambridge University Press.

Chamorro-Premuzic, Tomas, Dave Winsborough, Ryne A. Sherman, and Robert Hogan. 2016. “New Talent Signals: Shiny New Objects or a Brave New World?” *Industrial and Organizational Psychology* 9 (3): 621–40. https://doi.org/10.1017/iop.2016.6.

Chandler, Simon. 2017. “The AI Chatbot Will Hire You Now.” *Wired - The Big Story*, September 13. <https://www.wired.com/story/the-ai-chatbot-will-hire-you-now/>. (accessed 30.12.2024)

Chang, Cheng-chi (Kirin). 2024. “The First Global AI Treaty: Analyzing the Framework Convention on Artificial Intelligence and the Eu AI Act.” *University of Illinois Law Review Online* 2024 (Fall): 86–99. https://doi.org/10.2139/ssrn.5069335.

Chapman, Derek S., and David Mayers. 2018. “Recruitment Processes and Organizational Attraction.” In *Current Issues in Work and Organizational Psychology*. Routledge.

Chatgpt.com. 2025. “Https://Chatgpt.Com/.” <https://chatgpt.com/>. (accessed 23.4.2025)

Chaudhary, Mayuri. 2023. “ChatGPT in Human Resource Management.” *Spiceworks*, February 21. <https://www.spiceworks.com/hr/future-work/articles/chatgpt-can-be-a-game-changer-in-hrm/>. (accessed 19.11.2025)

Chen, Zhisheng. 2023. “Collaboration among Recruiters and Artificial Intelligence: Removing Human Prejudices in Employment.” *Cognition, Technology & Work* 25 (1): 135–49. https://doi.org/10.1007/s10111-022-00716-0.

Chen, Zhiyuan, and Bing Liu. 2018. *LIfelong Machine Learning*. 2nd ed. Synthesis Lectures on Artificial Intelligence and Machine Learning. Springer Cham. <https://doi.org/10.1007/978-3-031-01581-6>.

Cherry, Miriam A. 2016. “People Analytics and Invisible Labor The Law and Business of People Analytics.” *Saint Louis University Law Journal* 61 (1): 1–16.

Chopin, Isabelle, and Catharina Germaine. 2023. *A Comparative Analysis of Non-Discrimination Law in Europe 2022: The 27 EU Member States, Albania, Iceland, Liechtenstein, Montenegro,*

North Macedonia, Norway, Serbia, Turkey and the United Kingdom Compared. Publications Office. <https://data.europa.eu/doi/10.2838/428042>.

Chopra, Ankit. 2025. "Adoption of AI and Agentic Systems: Value, Challenges, and Pathways." *California Management Review*, August 15. <Adoption of AI and Agentic Systems: Value, Challenges, and Pathways>.

Christakis, Theodore. 2024. "AI Hallucinations and Data Subject Rights under the GDPR: Regulatory Perspectives and Industry Responses." SSRN Scholarly Paper No. 5042191. Social Science Research Network, December 2. <https://papers.ssrn.com/abstract=5042191>.

CJEU. 1991. "Opinion of the Court 1/91." Opinion. CJEU, December 14.

CJEU. 1995. *Report of the Court of Justice on Certain Aspects of the Application of the Treaty on European Union*. CJEU.

CJEU. 2011. "Opinion 1/09 of the Court." Opinion. August 3.

CJEU. 2014. "Opinion 2/13 of the Court." Opinion. December 18.

Clifford, Damian, and Jef Ausloos. 2018. "Data Protection and the Role of Fairness." *Yearbook of European Law* 37 (January): 130–87. https://doi.org/10.1093/yel/yey004.

CNIL. 2019. "Deliberation No. 2019-118 of 12 September 2019 for Adoption of the List of the Kind of Processing Operations for Which a Data Protection Impact Assessment Is Not Required."

Cobbe, Jennifer, and Jatinder Singh. 2021. "Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges." *Forthcoming in Computer Law & Security Review*, ahead of print. https://doi.org/10.2139/ssrn.3824736.

Cobbe, Jennifer, Michael Veale, and Jatinder Singh. 2023. "Understanding Accountability in Algorithmic Supply Chains." *2023 ACM Conference on Fairness Accountability and Transparency*, June 12, 1186–97. https://doi.org/10.1145/3593013.3594073.

Cofone, Ignacio N. 2018. "Algorithmic Discrimination Is an Information Problem." *Hastings Law Journal* 70 (6): 1389–444.

Cohen, Tammy. 2019. "How to Leverage Artificial Intelligence to Meet Your Diversity Goals." *Strategic HR Review* 18 (2): 62–65. https://doi.org/10.1108/SHR-12-2018-0105.

Conway, Gerard. 2012. *The Limits of Legal Reasoning and the European Court of Justice*. Studies in European Law and Policy. Cambridge University Press.

Cormen, Thomas H. 2009. "The Role of Algorithms in Computing." In *Introduction to Algorithms*, 3rd ed., by Thomas H. Cormen, Leiserson, Ronald L. Rivest, and Clifford Stein. MIT Press.

Countouris, Nicola, and Valerio De Stefano. 2019. *New Trade Union Strategies for New Forms of Employment*.

Criddle, Cristina, and Delphine Strauss. 2024. "Jobhunters Flood Recruiters with AI-Generated CVs." *Financial Times*, August 13. <https://www.ft.com/content/30a032dd-bdaa-4aee-bc51-754867abbde0?syn-25a6b1a6=1>. (accessed 21.11.2024)

Cristofolini, Chiara. 2024. "Navigating the Impact of AI Systems in the Workplace: Strengths and Loopholes of the EU AI Act from a Labour Perspective." *Italian Labour Law E-Journal* 17 (1): 1. https://doi.org/10.6092/issn.1561-8048/19796.

Custers, Bart, and Anne-Sophie Heijne. 2022. "The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice." *Computer Law & Security Review* 46 (September): 105727. https://doi.org/10.1016/j.clsr.2022.105727.

Custers, Bart, and Helena Vrabec. 2024. "Tell Me Something New: Data Subject Rights Applied to Inferred Data and Profiles." *Computer Law & Security Review* 52 (April): 105956. https://doi.org/10.1016/j.clsr.2024.105956.

CVViz. 2023. "AI Resume Screening | Automated Resume Screening Software | CVViZ." <https://cvviz.com/product/resume-screening/>. (accessed 19.11.2025)

Dale, Robert. 2021. “GPT-3: What’s It Good for?” *Natural Language Engineering* 27 (1): 113–18. https://doi.org/10.1017/S1351324920000601.

Dalenberg, David Jacobus. 2018. “Preventing Discrimination in the Automated Targeting of Job Advertisements.” *Computer Law & Security Review* 34 (3): 615–27. https://doi.org/10.1016/j.clsr.2017.11.009.

Daly, Patrick, and Darius Whelan. 2021. “Disability in Employment Equality Law: A Reappraisal of the Reasonable Accommodation Duty and Issues Arising in Its Implementation.” *Maastricht Journal of European and Comparative Law* 28 (6): 744–59. https://doi.org/10.1177/1023263X211035268.

Dastin, Jeffrey. 2018. “Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women.” *Reuters*, October 10. <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> (accessed 19.11.2025).

Datatilsynet. 2023. *Offentlige myndigheders brug af kunstig intelligens: Inden I går i gang*.

Davidov, Guy. 2016a. *A Purposive Approach to Labour Law*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198759034.001.0001.

Davidov, Guy. 2016b. “The Building Blocks of Labour Law: Employee and Employer.” In *A Purposive Approach to Labour Law*. Oxford University Press.

Davidov, Guy. 2017. “Subordination vs Domination: Exploring the Differences.” *International Journal of Comparative Labour Law and Industrial Relations* 33 (3). <https://doi.org/10.54648/ijcl2017016>.

Davies, A. C.L. 2012. *EU Labour Law*. Edward Elgar Publishing. https://doi.org/10.4337/9781781005156.

De Gregorio, Giovanni, and Simona Demkova. 2024. “The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe.” In *European Yearbook of Constitutional Law*, edited by C. van Oirsouw, J. de Poorter, I. Leijten, G. van der Schuff, and M. De Visser. Asser Press. <doi:10.1007/978-94-6265-647-5_10>.

De Hert, Paul, Serge Gutwirth, Anna Moscibroda, David Wright, and Gloria González Fuster. 2009. “Legal Safeguards for Privacy and Data Protection in Ambient Intelligence.” *Personal and Ubiquitous Computing* 13 (6): 435–44. https://doi.org/10.1007/s00779-008-0211-6.

De Hert, Paul, Vagelis Papakonstantinou, David Wright, and Serge Gutwirth. 2013. “The Proposed Regulation and the Construction of a Principles-Driven System for Individual Data Protection.” *Innovation: The European Journal of Social Science Research* 26 (1–2): 133–44. https://doi.org/10.1080/13511610.2013.734047.

De Stefano, Valerio, and Mathias Wouters. 2022. “AI and Digital Tools in Workplace Management and Evaluation: An Assessment of the EU’s Legal Framework.” SSRN Scholarly Paper No. 4144899. Rochester, NY, March 1. <https://papers.ssrn.com/abstract=4144899>.

De Vos, Marc. 2020. “The European Court of Justice and the March towards Substantive Equality in European Union Anti-Discrimination Law.” *International Journal of Discrimination and the Law* 20 (1): 62–87. https://doi.org/10.1177/1358229120927947.

Deakin, S. 2001. “Commentary. The Changing Concept of the ‘employer’ in Labour Law.” *Industrial Law Journal* 30 (1): 72–84. https://doi.org/10.1093/ilj/30.1.72.

DeepSeek-AI, Aixin Liu, Bei Feng, et al. 2025. “DeepSeek-V3 Technical Report.” arXiv:2412.19437. Preprint, arXiv, February 18. <http://arxiv.org/abs/2412.19437>.

Demkova, Simona. 2024. “The AI Act’s Right to Explanation: A Plea for an Integrated Remedy.” *MediaLaws*, October 31. <https://www.medialaws.eu/the-ai-acts-right-to-explanation-a-plea-for-an-integrated-remedy/>.

Desouza, Kevin C., Gregory S. Dawson, and Daniel Chenok. 2020. "Designing, Developing, and Deploying Artificial Intelligence Systems: Lessons from and for the Public Sector." *Business Horizons*, Artificial Intelligence and Machine Learning, vol. 63 (2): 205–13. https://doi.org/10.1016/j.bushor.2019.11.004.

Dimitrova, Diana. 2020. "The Right to Explanation under the Right of Access to Personal Data: Legal Foundations in and beyond the GDPR." *European Data Protection Law Review (EDPL)* 6 (2): 211–30.

Domingos, Pedro. 2012. "A Few Useful Things to Know About Machine Learning." *Communications of the ACM* 55 (10): 78–87. https://doi.org/10.1145/2347736.2347755.

Dong, Yi, Ronghui Mu, Yanghao Zhang, et al. 2024. "Safeguarding Large Language Models: A Survey." arXiv:2406.02622. Preprint, arXiv, June 3. <http://arxiv.org/abs/2406.02622>.

Doroga, Sorina, and Alexandra Mercescu. 2021. "A Call to Impossibility : The Methodology of Interpretation at the European Court of Justice and the PSPP Ruling." *European Journal of Legal Studies* (IT), no. 2 (November). https://doi.org/10.2924/EJLS.2021.006.

Douglas-Scott, Sionaidh, and Nicholas Hatzis, eds. 2017. *Research Handbook on EU Law and Human Rights*. 1st ed. Edward Elgar Publishing.

Dreyer, Stephan, and Wolfgang Schulz. 2019. *The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?: Potentials and Limitations in Ensuring the Rights and Freedoms of Individuals, Groups and Society as a Whole*. Discussion Paper Ethics of Algorithms No. 5. Version 1. BStift - Bertelsmann Stiftung. <https://www.bertelsmann-stiftung.de/doi/10.11586/2018018>.

Drouard, Etienne, Olga Kurochkina, Rémy Schlich, and Daghan Ozturk. 2024a. "The Interplay between the AI Act and the GDPR: Part I - When and How to Comply with Both." *Journal of AI Law and Regulation* 1 (2): 164–76. https://doi.org/10.21552/aire/2024/2/4.

Drouard, Etienne, Olga Kurochkina, Rémy Schlich, and Daghan Ozturk. 2024b. "The Interplay between the AI Act and the GDPR: Part II - Compliance Challenges for AI Systems That Use Personal Data." *Journal of AI Law and Regulation* 1 (3): 297–309. https://doi.org/10.21552/aire/2024/3/6.

Dubal, Veena. 2025. "Data Laws at Work." *Yale Law Journal Forum*, January, 405–47.

Duboust, Oceane. 2025. "More than 3 out of 4 Workers Have Already Used AI in Their Job Search, New Survey Finds." Euronews, January 29. <https://www.euronews.com/next/2025/01/29/more-than-3-out-of-4-workers-have-already-used-ai-in-their-job-search-new-survey-finds>. (accessed 4.4.2025)

Duunitori. 2024. *Kansallinen rekrytointitutkimus 2024*. Helsinki. <www.rekrytointitutkimus.fi>. (accessed 5.9.2025)

Ebers, Martin. 2021. "Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act." SSRN Scholarly Paper No. 3900378. Rochester, NY, August 6. https://doi.org/10.2139/ssrn.3900378.

Ebers, Martin. 2024. "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act." *European Journal of Risk Regulation*, November 6, 1–20. https://doi.org/10.1017/err.2024.78.

EDPB. 2018a. "Endorsement 1/2018 of WP29 Documents." EDPB, May 25.

EDPB. 2018b. "Opinion 1/2018 on the Draft List of the Competent Supervisory Authority of Austria Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR)." September 25.

EDPB. 2018c. “Opinion 12/2018 on the Draft List of the Competent Supervisory Authority of Italy Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR).” September 25.

EDPB. 2018d. “Opinion 13/2018 on the Draft List of the Competent Supervisory Authority of Lithuania Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR).” September 25.

EDPB. 2019a. “Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects, Version 2.0.” European Data Protection Board, August 10.

EDPB. 2019b. “Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3), Version 2.1.” December 11.

EDPB. 2019c. “Opinion 01/2019 on the Draft List of the Competent Supervisory Authority of the Principality of Liechtenstein Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR).” January 23.

EDPB. 2020a. “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0.” EDPB, October 20.

EDPB. 2020b. “Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR (Part 1) - Version 2.0.” EDPB, July 7.

EDPB. 2020c. “Guidelines 05/2020 on Consent under Regulation 2016/679, Version 1.1, Adopted on 4 May 2020.” European Data Protection Board.

EDPB. 2020d. “Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre | European Data Protection Board.” EDPB, February 10. <https://www.edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en>.

EDPB. 2021. “Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR.” EDPB, July 7.

EDPB. 2023. “Guidelines 01/2022 on Data Subject Rights - Right of Access.” EDPB, March 28.

EDPB. 2024a. “Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR.” EDPB, August 10.

EDPB. 2024b. “Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models.” EDPB, December 17.

EDPB. 2024c. “Report of the Work Undertaken by the ChatGPT Taskforce.” EDPB, May 23.

EDPB. 2026. “FAQ | European Data Protection Board.” September 2. <https://www.edpb.europa.eu/sme-data-protection-guide/faq-search_en?search=consent>.

EDPB, and EDPS. 2021. “Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).” European Data Protection Board & European Data Protection Supervisor, June 18.

EDPS. 2017. “Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit.” European Data Protection Supervisor, November 4. <https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf>.

EDPS. 2024. “EDPS Comments to the AI Office’s Consultation on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act Launched by the European AI Office.” December 19. <https://www.edps.europa.eu/system/files/2025-01/2024-12-18_submission_ai_board_on_prohibitions_en.pdf>.

EDPS. 2025. “Generative AI and the EUDPR. Orientations for Ensuring Data Protection Compliance When Using Generative AI Systems. (Version 2).” October 28. <https://www.edps.europa.eu/system/files/2025-10/25-10_28_revised_genai_orientations_en.pdf>.

Edwards, Lilian, and Michael Veale. 2017. “Slave to the Algorithm? Why a ‘right to an Explanation’ Is Probably Not the Remedy You Are Looking For.” *Duke Law & Technology Review* 16 (1): 18–84. https://doi.org/10.31228/osf.io/97upg.

Eecke, Patrick van, and Bartholomäus Regenhard. 2024. “Article 1 - Subject Matter.” In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Eklund, Mia. 2021. “Integritet och övervakning i arbetslivet – juridiska perspektiv på arbetsgivarens rätt att övervaka arbetstagare.” Doctoral dissertation, University of Helsinki.

Elearn. 2009. *Recruitment and Selection*. Rev. ed. Elsevier : eLearn.

Ellis, Evelyn, and Philippa Watson. 2012. *EU Anti-Discrimination Law*. 2nd ed. Oxford University Press.

Enarsson, Therese, Lena Enqvist, and Markus Naarttijärvi. 2022. “Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts.” *Information & Communications Technology Law* 31 (1): 123–53. https://doi.org/10.1080/13600834.2021.1958860.

Engel, Andreas, Philipp Hacker, and Marco Mauer. 2023. “Technical Report (Annex to Regulating ChatGPT and Other Large Generative AI Models).” Paper presented at 2023 ACM Conference on Fairness, Accountability, and Transparency.

Engelen, Jesper E. van, and Holger H. Hoos. 2020. “A Survey on Semi-Supervised Learning.” *Machine Learning* 109 (2): 373–440. https://doi.org/10.1007/s10994-019-05855-6.

Ervasti, Kaijus. 2000. “Empirisk Forskning, Rättsvetenskap Och Rättens Dynamiska Element.” *JFT*, no. 6.

EUR-Lex. 2026. “The Direct Effect of European Union Law | EUR-Lex.” EUR-Lex. <https://eur-lex.europa.eu/EN/legal-content/summary/the-direct-effect-of-european-union-law.html>.

European Artificial Intelligence Office. 2025. “Living Repository of AI Literacy Practices.” April 16.

European Commission. 2025a. “Annexes to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Commission Work Programme 2025.”

European Commission. 2025b. “Commission Collects Feedback to Simplify Rules on Data, Cybersecurity and Artificial Intelligence in the Upcoming Digital Omnibus.” European Commission - Shaping Europe’s Digital Future, September 16. <https://digital-strategy.ec.europa.eu/en/news/commission-collects-feedback-simplify-rules-data-cybersecurity-and-artificial-intelligence-upcoming>.

European Commission. 2025c. “Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act).” April 2.

European Commission. 2025d. “Commission Guidelines on the Definition of an Artificial Intelligence System Established by Regulation (EU) 2024/1689 (AI Act).” European Commission.

European Commission. 2025e. “Draft Guidance Article 73 AI Act- Incident Reporting (High-Risk AI Systems).” September 26. <https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks>.

European Commission. 2026. “Standardisation of the AI Act.” Shaping Europe’s Digital Future, March 19. <https://digital-strategy.ec.europa.eu/en/policies/ai-act-standardisation>.

European Employment Services, (EURES). 2024. *How AI Can Improve the Talent Acquisition Process - European Union*. December 9. <https://eures.europa.eu/how-ai-can-improve-talent-acquisition-process-2024-09-12_en>.

European Union Agency for Fundamental Rights. 2020. *Getting the Future Right – Artificial Intelligence and Fundamental Rights*. European Union Agency for Fundamental Rights.

European Union Agency for Fundamental Rights. 2024. *GDPR in Practice - Experiences of Data Protection Authorities*. European Union Agency for Fundamental Rights.

Expert Group on Liability and New Technologies - New Technologies Formation. 2019. *Liability for Artificial Intelligence and Other Emerging Digital Technologies.Pdf*. European Union. <doi:10.2838/573689>.

Fabris, Alessandro, Nina Baranowska, Matthew J. Dennis, et al. 2024. "Fairness and Bias in Algorithmic Hiring: A Multidisciplinary Survey." arXiv:2309.13933. Preprint, arXiv, April 8. <http://arxiv.org/abs/2309.13933>.

Faliagka, Evanthia, Lazaros Iliadis, Ioannis Karydis, et al. 2014. "On-Line Consistent Ranking on e-Recruitment: Seeking the Truth behind a Well-Formed CV." *The Artificial Intelligence Review* 42 (3): 515–28. https://doi.org/http://dx.doi.org/10.1007/s10462-013-9414-y.

Feiler, Lukas, and Beat König. 2024. "Article 3 - Definitions." In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Fennelly, Nial. 1996. "Legal Interpretation at the European Court of Justice." *Fordham International Law Journal* 20 (3): 656.

Fernandes, Elora, Wayne Holmes, and Sopio Zhgenti. 2024. "Article 4 - AI Literacy." In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Ferrajoli, Luigi. 2001. "Fundamental Rights." *International Journal for the Semiotics of Law* 14: 1–33.

Ferretly. 2025. "Home - Ferretly - AI-Powered Social Media Screening." <https://www.ferretly.com/>.

Feuerriegel, Stefan, Jochen Hartmann, Christian Janiesch, and Patrick Zschech. 2024. "Generative AI." *Business & Information Systems Engineering* 66 (1): 111–26. https://doi.org/10.1007/s12599-023-00834-7.

Fink, Melanie. 2025. "The Hidden Reach of the EU AI Act." *Verfassungsblog*, ahead of print, January 20. https://doi.org/10.59704/266732ab11c973f4.

Finnish Data Protection Ombudsman. 2024. *Annual Report of the Office of the Data Protection Ombudsman of Finland 2024*. (Helsinki).

Fontanelli, Filippo. 2014. "The Implementation of European Union Law by Member States under Article 51(1) of the Charter of Fundamental Rights." *Columbia Journal of European Law* 20 (3).

Fornasier, Matteo. 2015. "The Impact of EU Fundamental Rights on Private Relationships: Direct or Indirect Effect?" *European Review of Private Law* 23 (May): 29–46.

Fourney, Adam, Gagan Bansal, Hussein Mozannar, et al. 2024. "Magentic-One: A Generalist Multi-Agent System for Solving Complex Tasks." arXiv:2411.04468. Preprint, arXiv, November 7. <http://arxiv.org/abs/2411.04468>.

Frantziou, Eleni. 2019. "(Most of) the Charter of Fundamental Rights Is Horizontally Applicable: ECJ 6 November 2018, Joined Cases C-569/16 and C-570/16, Bauer et Al." *European Constitutional Law Review* 15 (2): 306–23. https://doi.org/10.1017/S1574019619000166.

Fredman, Sandra. 2016. "Substantive Equality Revisited." *International Journal of Constitutional Law* 14 (3): 712–38. https://doi.org/10.1093/icon/mow043.

Fredman, Sandra. 2022. *Discrimination Law*. 3rd ed. Oxford University Press. https://doi.org/10.1093/oso/9780198854081.003.0005.

Fülop, Tünde, and Philipp Poindl. 2024. "Article 27 - Fundamental Rights Impact Assessment for High-Risk AI Systems." In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Gadbled, Robin, and Elise Muir. 2022. "Actors and Roles in EU Law: Asking 'Who Does What?' In the European Union Legal System." *European Constitutional Law Review* 18 (4): 621–36. https://doi.org/10.1017/S1574019622000426.

Gallagher, Daniel. 2024. "Article 26 - Obligations of Deployers of High-Risk AI Systems." In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Gan, Chengguang, Qinghao Zhang, and Tatsunori Mori. 2024. "Application of LLM Agents in Recruitment: A Novel Framework for Resume Screening." arXiv:2401.08315. Preprint, arXiv, August 13. <http://arxiv.org/abs/2401.08315>.

Gao, Yunfan, Yun Xiong, Xinyu Gao, et al. 2024. "Retrieval-Augmented Generation for Large Language Models: A Survey." arXiv:2312.10997. Preprint, arXiv, March 27. https://doi.org/10.48550/arXiv.2312.10997.

Gaucher, Danielle, Justin Friesen, and Aaron C. Kay. 2011. "Evidence That Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality." *Journal of Personality and Social Psychology* 101 (1): 109–28. 2011-04642-001. https://doi.org/10.1037/a0022530.

Gaudeul, Alexia, Ottla Arrigoni, Vasiliki Charisi, Marina Escobar-Planas, and Isabelle Hupont. 2024. *The Impact of Human Oversight on Discrimination in AI-Supported Decision-Making: A Large Case Study on Human Oversight of AI Based Decision Support Systems in Lending and Hiring Scenarios.* Publications Office. <https://data.europa.eu/doi/10.2760/0189570>.

Gaudio, Giovanni. 2023. *Litigating the Algorithmic Boss in the EU: A (Legally) Feasible and (Strategically) Attractive Option for Trade Unions?*

Gavaghan, Colin, Alistair Knott, and James Maclaurin. 2021. *The Impact of Artificial Intelligence on Jobs and Work in New Zealand*. Final Report on Phase 2 of the Artificial Intelligence and Law in New Zealand Project. University of Otago.

Gellert, Raphaël. 2021. "The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?" *Journal of Ethics and Legal Technologies* (Padova, IT) 3 (2): 15–33. https://doi.org/10.14658/pupj-jelt-2021-2-2.

Gender Decoder. 2025. "Gender Decoder: Find Subtle Bias in Job Ads." <https://gender-decoder.katmatfield.com/>.

Genicot, Nathan. 2025. "Scoring the European Citizen in the AI Era." *Computer Law & Security Review* 57 (July): 106130. https://doi.org/10.1016/j.clsr.2025.106130.

Georgieva, Ludmila. 2020. "Article 10. Processing of Personal Data Relating to Criminal Convictions and Offences." In *The EU General Data Protection Reuglation (GDPR): A Commentary*, 1st ed., edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Gerards, Janneke, and Frederik Zuiderveen Borgesius. 2022. "Protected Grounds and the System of Non-Discrimination Law in the Context of Algorithmic Decision-Making and Artificial Intelligence Articles and Essays." *Colorado Technology Law Journal* 20 (1): 1–56.

Gerards, Janneke, and Raphaële Xenidis. 2020. *Algorithmic Discrimination in Europe: Challenges and Opportunities for Gender Equality and Non-Discrimination Law.* <https://data.europa.eu/doi/10.2838/544956>.

Gerrish, Sean. 2018. *How Smart Machines Think*. The MIT Press.

Gershgorn, Greg. 2018. "Companies Are on the Hook If Their Hiring Algorithms Are Biased." Quartz, October 22. <https://qz.com/1427621/companies-are-on-the-hook-if-their-hiring-algorithms-are-biased/>. (accessed 7.12.2024)

Gervais, Daniel J., Noam Shemtov, Haralambos Marmanis, and Catherine Zaller Rowland. 2024. "The Heart of the Matter: Copyright, AI Training, and LLMs." SSRN Scholarly Paper No. 4963711. Social Science Research Network, September 21. https://doi.org/10.2139/ssrn.4963711.

Gestel, Rob van, and Hans-Wolfgang Micklitz. 2011. "Revitalising Doctrinal Legal Research in Europe: What About Methodology?" In *European Legal Method - Paradoxes and Revitalisation*, edited by Ulla Neergaard, Ruth Nielsen, and Lynn Roseberry. DJOF Publishing.

Gestel, Rob van, and Hans-Wolfgang Micklitz. 2014. "Why Methods Matter in European Legal Scholarship." *European Law Journal* 20 (3): 292–316. https://doi.org/10.1111/eulj.12049.

Giermindl, Lisa Marie, Franz Strich, Oliver Christ, Ulrich Leicht-Deobald, and Abdullah Redzepi. 2022. "The Dark Sides of People Analytics: Reviewing the Perils for Organisations and Employees." *European Journal of Information Systems* 31 (3): 410–35. https://doi.org/10.1080/0960085X.2021.1927213.

Gikopoulos, John. 2019. "Alongside, Not against: Balancing Man with Machine in the HR Function." *Strategic HR Review* 18 (2): 56–61. https://doi.org/10.1108/SHR-12-2018-0103.

Gillespie, Nicole, Steven Lockey, Tabi Ward, Alexandria Macdade, and Gerard Hassed. 2025. *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025*. The University of Melbourne. 4974511 Bytes. https://doi.org/10.26188/28822919.

Gils, Thomas. 2024. "Article 50 - Transparency Obligations for Providers and Deployers of Certain AI Systems." In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Glaser, Barney G., and Anselm L. Strauss. 1968. *Discovery of Grounded Theory*. Weidenfeld and nicolson.

Gohire.io. 2025. "Free Job Description Generator." Gohire. <https://gohire.io/free-job-description-generator>. (accessed 26.3.2025)

Goktas, Polat. 2024. "Ethics, Transparency, and Explainability in Generative Ai Decision-Making Systems: A Comprehensive Bibliometric Study." *Journal of Decision Systems*, October 10, 1–29. https://doi.org/10.1080/12460125.2024.2410042.

Graham, Logan, Abigail Gilbert, Joshua Simons, and Anna Thomas. 2020. *Artificial Intelligence in Hiring - Assessing Impacts on Equality*. Institute for the Future of Work (IFOW).

Gramano, Elena. 2024. "Nothing, Yet Everything New Under the Sun: Subordination, Authority, and Transformations of the Organization Work in a Labor Law Perspective." *Comparative Labor Law & Policy Journal* 44 (3): 305–26.

Grammarly.com. 2025. "Grammarly: Free AI Writing Assistance." <https://www.grammarly.com/>. (accessed 23.4.2025)

Greenberg, Andy. 2025. "McDonald's AI Hiring Bot Exposed Millions of Applicants' Data to Hackers Who Tried the Password '123456.'" Tags. *Wired*, September 7. <https://www.wired.com/story/mcdonalds-ai-hiring-chat-bot-paradoxai/>. (accessed 4.10.2025)

Greif, Elisabeth, and Tessa Grosz. 2023. "To See, or Not to See: Online Job Advertisement and EU Non-Discrimination Law." *European Labour Law Journal* 14 (3): 376–90. https://doi.org/10.1177/20319525231172089.

Grimmelmann, James, and Daniel Westreich. 2017. “Incomprehensible Discrimination.” *Cornell Law Review Online* 7 (164): 164–77. https://doi.org/10.15779/Z38707WN47.

Grozdanovski, Ljupcho. 2021. “In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law.” *Common Market Law Review* 58 (1): 99–136.

Grozdanovski, Ljupcho. 2025. “Non-Discrimination Law, the GDPR, the AI Act and the - Now Withdrawn - AI Liability Directive Proposal Offering Gateways to Pre-Trial Knowledge of Algorithmic Discrimination.” *AI and Ethics*, May 29, 1–24. https://doi.org/10.1007/s43681-025-00754-0.

Grzankowski, Alex, Stephen M. Downes, and Partick Forber. 2025. “LLMs Are Not Just next Token Predictors.” *Inquiry*, January 12, 1–11. https://doi.org/10.1080/0020174X.2024.2446240.

Gstrein, Oskar J., Noman Haleem, and Andrej Zwitter. 2024. “General-Purpose AI Regulation and the European Union AI Act.” *Internet Policy Review* 13 (3): 1–26. https://doi.org/10.14763/2024.3.1790.

Guihot, Michael, Anne F. Matthew, and Nicolas P. Suzor. 2017. “Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence.” *Vanderbilt Journal of Entertainment & Technology Law* 20 (2): 385–456.

Guinness, Harry. 2024. *The Best Large Language Models (LLMs) in 2024*. May 8. <https://zapier.com/blog/best-llm/>.

Hacker, Philipp. 2018. “Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law.” *Common Market Law Review* 55 (4): 1143–86.

Hacker, Philipp. 2021. “A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act.” *Law, Innovation and Technology* 13 (2): 257–301. https://doi.org/10.1080/17579961.2021.1977219.

Hacker, Philipp. 2024a. “Comments on the Final Trilogue Version of the AI Act.” SSRN Scholarly Paper No. 4757603. Rochester, NY, January 23. https://doi.org/10.2139/ssrn.4757603.

Hacker, Philipp. 2024b. “Sustainable AI Regulation.” *Common Market Law Review* 61 (2). <https://doi.org/10.54648/cola2024025>.

Hacker, Philipp. 2024c. *The AI Act between Digital and Sectoral Regulations*. https://doi.org/10.11586/2024188.

Hacker, Philipp, Johann Cordes, and Janina Rochon. 2022. “Regulating Gatekeeper AI and Data: Transparency, Access, and Fairness under the DMA, the GDPR, and Beyond.” *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.4316944.

Hacker, Philipp, Andreas Engel, Sarah Hammer, and Brent Mittelstadt. 2025. “Introduction to the Foundations and Regulation of Generative AI.” SSRN Scholarly Paper No. 5137750. Social Science Research Network, February 14. <https://papers.ssrn.com/abstract=5137750>.

Hacker, Philipp, Andreas Engel, and Marco Mauer. 2023. “Regulating ChatGPT and Other Large Generative AI Models.” *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA), FAccT ’23, June 12, 1112–23. https://doi.org/10.1145/3593013.3594067.

Hagendorff, Thilo. 2020. “The Ethics of AI Ethics: An Evaluation of Guidelines.” *Minds and Machines* 30 (1): 99–120. https://doi.org/10.1007/s11023-020-09517-8.

Halila, Heikki. 2015. “Oikeustieteellinen väitöskirja ennen ja nyt.” *Lakimies*, nos. 7–8: 1108–30.

Hamburg Commissioner for Data protection and freedom of information. 2024. “Discussion Paper: Large Language Models and Personal Data.”

Hao, Shibo, Sainbayar Sukhbaatar, DiJia Su, et al. 2024. “Training Large Language Models to Reason in a Continuous Latent Space.” arXiv:2412.06769. Preprint, arXiv, December 11. <http://arxiv.org/abs/2412.06769>.

Harbo, Tor-Inge. 2010. “The Function of the Proportionality Principle in EU Law.” *European Law Journal* 16 (2): 158–85. https://doi.org/10.1111/j.1468-0386.2009.00502.x.

Hartkamp, Arthur. 2013. “The Concept of (Direct and Indirect) Horizontal Effect of EU Law: The Terminology of European Law Scholars and of Private Law Scholars Compared.” In *General Principles of EU Law and European Private Law*. European Monographs 84. Kluwer Law International BV.

He, Ran, Jie Cao, and Tieniu Tan. 2025. “Generative Artificial Intelligence: A Historical Perspective.” *National Science Review* 12 (5). https://doi.org/10.1093/nsr/nwaf050.

Heaven, Will Douglas. 2023. “GPT-4 Is Bigger and Better than ChatGPT—but OpenAI Won’t Say Why.” *MIT Technology Review*, March 14. <https://www.technologyreview.com/2023/03/14/1069823/gpt-4-is-bigger-and-better-chatgpt-openai/>.

Hendrickx, Frank. 2018. “Regulating New Ways of Working: From the New ‘Wow’ to the New ‘How.’” *European Labour Law Journal* 9 (2): 195–205. https://doi.org/10.1177/2031952518781449.

Hermanns, Holger, Anne Lauber-Rönsberg, Philip Meinel, Sarah Sterz, and Hanwei Zhang. 2024. “AI Act for the Working Programmer.” arXiv:2408.01449. Preprint, arXiv, July 23. https://doi.org/10.48550/arXiv.2408.01449.

Hesselink, Martijn W. 2011. “A Toolbox for European Judges.” In *European Legal Method - Paradoxes and Revitalisation*, edited by Ulla Neergaard, Ruth Nielsen, and Lynn Roseberry. DJOF Publishing.

Hettne, Jörgen, Ida Otken Eriksson, Vladimir Bastidas Venegas, Xavier Groussot, Jane Reichel, and Maria Bergström. 2011. *EU-rättslig metod - Teori och genomslag i svensk rättstillämpning*. 2nd ed. Edited by Jörgen Hettne and Ida Otken Eriksson. Norstedts Juridik AB.

Heymans, Juma. 2024. *How to Use LLMs in Recruitment - a Practical Guide*. April 26. <https://www.herohunt.ai/blog/how-to-use-llms-in-recruitment>. (accessed 25.9.2024)

Hijmans, Hielke. 2020. “Article 1. Subject-Matter and Objectives.” In *The EU General Data Protection Reuglation (GDPR): A Commentary*, 1st ed., edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Hildebrandt, Mireille. 2015. *Smart Technologies and the End(s) of Law*. Edward Elgar Publishing. https://doi.org/10.4337/9781849808774.

Hireright. 2025. “Social Media Search & Background Check Service.” <https://www.hireright.com/en-EMEA/services/social-media-search>. (accessed 27.3.2025)

HireVue. 2023. “HireVue Hiring Platform: Video Interviews, Assessments, AI, and More.” <https://www.hirevue.com/> (accessed 16.3.2025).

Hirize. 2024. *Revolutionizing Recruitment: How LLMs Transform Recruiting | Hirize*. <https://hirize.ai>. (accessed 27.11.2024)

Hoecke, Mark van. 2013. “Legal Doctrine: Which Method(s) for What Kind of Discipline?” In *Methodologies of Legal Research : Which Kind of Method for What Kind of Discipline?* Bloomsbury Publishing.

Hohfeld, Wesley Newcomv. 1913. “Some Fundamental Legal Conceptions as Applied in Judicial Reasoning.” *Yale Law Journal* 23 (1): 16–59.

Horodyski, Piotr. 2023. "Recruiter's Perception of Artificial Intelligence (AI)-Based Tools in Recruitment." *Computers in Human Behavior Reports* 10 (May): 100298. https://doi.org/10.1016/j.chbr.2023.100298.

Houser, Kimberly A. 2019. *Can AI Solve the Diversity Problem in the Tech Industry? Mitigating Noise and Bias in Employment Decision-Making*. 65.

Hu, Krystal, and Krystal Hu. 2023. "ChatGPT Sets Record for Fastest-Growing User Base - Analyst Note." Technology. *Reuters*, February 2. <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>. (accessed 23.4.2025)

Huang, Lei, Weijiang Yu, Weitao Ma, et al. 2024. "A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions." *ACM Trans. Inf. Syst.*, ahead of print, November 20. https://doi.org/10.1145/3703155.

Humanly. 2025. "Screen with Efficiency and Precision | Humanly." Humanly. <https://humanly.io>. (accessed 26.3.2025)

Hunkenschroer, Anna Lena, and Alexander Kriebitz. 2023. "Is AI Recruiting (Un)Ethical? A Human Rights Perspective on the Use of AI for Hiring." *AI and Ethics* 3 (1): 199–213. https://doi.org/10.1007/s43681-022-00166-4.

Hunkenschroer, Anna Lena, and Christoph Luetge. 2022. "Ethics of AI-Enabled Recruiting and Selection: A Review and Research Agenda." *Journal of Business Ethics* 178 (4): 977–1007. https://doi.org/10.1007/s10551-022-05049-6.

Hutchinson, Terry, and Nigel Duncan. 2012. "Defining and Describing What We Do: Doctrinal Legal Research." *Deakin Law Review* 17 (1): 83–120.

IBM Research. 2023. "What Is Retrieval-Augmented Generation (RAG)?" IBM Research, August 22. <https://research.ibm.com/blog/retrieval-augmented-generation-RAG>. (accessed 19.12.2024)

ICO. 2021. "What Is Criminal Offence Data?" ICO. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/criminal-offence-data/what-is-criminal-offence-data/#whatis>.

ICO. 2023. "ICO Guidance on AI and Data-Protection 2.0." <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection-2-0.pdf>.

ICO. 2024. "AI Tools in Recruitment - Audit Outcomes Report." <https://ico.org.uk/media/about-the-ico/documents/4031620/ai-in-recruitment-outcomes-report.pdf>.

Imana, Basileal, Aleksandra Korolova, and John Heidemann. 2021. "Auditing for Discrimination in Algorithms Delivering Job Ads." *Proceedings of the Web Conference 2021*, April 19, 3767–78. https://doi.org/10.1145/3442381.3450077.

Integritetsskydds myndigheten (IMY). 2025. *Årsredovisning 2024*. Integritetsskydds myndigheten (IMY).

Ji, Jessica, Josh A. Goldstein, and Andrew J. Lohn. 2023. "Controlling Language Model Outputs - A Primer." Center for Security and Emerging Technology.

Job Description.ai. 2023. "Job Description Generator Using AI | Job Description AI." <https://jobdescription.ai/>. (accessed 26.3.2025)

Jobilla. 2025. "Recruitment Software & Hiring Tools | Jobilla Products Overview." <https://www.jobilla.com/products>. (accessed 26.3.2025)

JOBMA. 2025. "Virtual Interviewing Platform | Video Interviews, Assessments, AI." JOBMA. <https://www.jobma.com>. (accessed 26.3.2025)

Jones, Katherine. 2024. "Top AI Recruiting Tools and Software of 2024." *TechTarget*, January. (accessed 28.11.2024)

Jordan, M. I., and T. M. Mitchell. 2015. “Machine Learning: Trends, Perspectives, and Prospects.” *Science* 349 (6245): 255–60. https://doi.org/10.1126/science.aaa8415.

Jotform. 2025. “Candidate Questionnaire AI Agent Template.” Jotform. <https://eu.jotform.com/agent-templates/candidate-questionnaire-ai-agent>. (accessed 26.3.2025)

Joveo. 2025. “Job Description Optimizer.” Joveo. <https://www.joveo.com/job-description-optimizer/>. (accessed 26.3.2025)

Kamarinou, Dimitra, Christopher Millard, and Jatinder Singh. 2016. “Machine Learning with Personal Data.” *Queen Mary University of London, School of Law Legal Studies Research Paper* 247: 1–23.

Kambhampati, Subbarao, Kaya Stechly, and Karthik Valmeekam. 2025. “(How) Do Reasoning Models Reason?” arXiv:2504.09762. Preprint, arXiv, May 27. <http://arxiv.org/abs/2504.09762>.

Kaminski, Margot E. 2019. “The Right to Explanation, Explained.” *Berkeley Technology Law Journal* 34: 189–218. https://doi.org/https://doi.org/10.15779/Z38TD9N83H.

Kaminski, Margot E, and Gianclaudio Malgieri. 2021. “Algorithmic Impact Assessments under the GDPR: Producing Multi-Layered Explanations.” *International Data Privacy Law* 11 (2): 20.

Kammerer, Brittany. 2021. “Hired by a Robot: The Legal Implications of Artificial Intelligence Video Interviews and Advocating for Greater Protection of Job Applicants Notes.” *Iowa Law Review* 107 (2): 817–50.

Kangas, Urpo. 1982. *Lesken oikeudellinen asema. Oikeusdogmaattinen tutkimus lesken sosiaaliturvan laajuudesta.* Suomalaisen Lakimiesyhdistyksen julkaisuja, A-sarja 156. Suomalainen Lakimiesyhdistys.

Kangas, Urpo. 1997. “Minun metodini.” In *Minun metodini*, edited by Juha Häyhä. Werner Söderström Lakitieto Oy.

Kaplan, Jared, Sam McCandlish, Tom Henighan, et al. 2020. “Scaling Laws for Neural Language Models.” arXiv:2001.08361. Preprint, arXiv, January 23. https://doi.org/10.48550/arXiv.2001.08361.

Keller, Milla. 2025. *Datajuridiikka - Paremmat Pelisäännöt Datataloudelle.* Alma Insights.

Kelly-Lyth, Aislinn. 2021. “Challenging Biased Hiring Algorithms.” *Oxford Journal of Legal Studies* 41 (4): 899–928. https://doi.org/10.1093/ojls/gqab006.

Kelly-Lyth, Aislinn. 2023. “Algorithmic Discrimination at Work.” *European Labour Law Journal* 14 (2): 152–71. https://doi.org/10.1177/20319525231167300.

Kelsey-Sugg, Anna, and Damien Carrick. 2024. “When AI Wrongly Described This Man as a Criminal, It Thrust Him into Uncharted Legal Territory.” *ABC News*, November 3. <https://www.abc.net.au/news/2024-11-04/ai-artificial-intelligence-hallucinations-defamation-chatgpt/104518612>. (accessed 19.12.2024)

Keppeler, Florian. 2024. “No Thanks, Dear AI! Understanding the Effects of Disclosure and Deployment of Artificial Intelligence in Public Sector Recruitment.” *Journal of Public Administration Research and Theory* 34 (1): 39–52. https://doi.org/10.1093/jopart/muad009.

Kim, Pauline T. 2017. “Data-Driven Discrimination at Work.” *William & Mary Law Review* 58 (3): 857–936.

Kim, Pauline T, and Sharion Scott. 2018. “Discrimination in Online Employment Recruiting.” *Saint Louis University Law Journal* 63 (1): 93–118.

Kindt, Els J., and Catherine Jasserand. 2024. “Article 5 - Prohibited AI Practices.” In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Klein, Naomi. 2023. “AI Machines Aren’t ‘Hal-lu-cin-at-ing’. But Their Makers Are.” *The Guardian Australia*, September 5.

Kleinberg, Jon, Jens Ludwig, Sendhil Mullainathan, and Cass R. Sunstein. 2018. "Discrimination in the Age of Algorithms." *Journal of Legal Analysis* 10 (1): 113–74. https://doi.org/10.1093/jla/laz001.

Klimas, Tadas, and Jūratė Vaičiukaitė. 2008. "The Law of Recitals in European Community Legislation." *ILSA Journal of International and Comparative Law* 15 (1): 33.

Köchling, Alina, and Marius Claus Wehner. 2020. "Discriminated by an Algorithm: A Systematic Review of Discrimination and Fairness by Algorithmic Decision-Making in the Context of HR Recruitment and HR Development." *Business Research* 13 (3): 795–848. https://doi.org/10.1007/s40685-020-00134-w.

Koivisto, Ida. 2015. Oikeus on, Miten Se Systematisoidaan? – Kysymys Oikeudenalajaotuksesta Ja Hallinto- Oikeudesta. *Lakimies* nos. 7–8: 954–72.

Komárek, Jan. 2015. "Legal Reasoning in EU Law." In *The Oxford Handbook of European Union Law*, edited by Damian Chalmers and Anthony Arnull. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199672646.013.3.

Kong, Yeqing, and Huiling Ding. 2024. "Tools, Potential, and Pitfalls of Social Media Screening: Social Profiling in the Era of AI-Assisted Recruiting." *Journal of Business and Technical Communication* 38 (1): 33–65. https://doi.org/10.1177/10506519231199478.

Kosinski, Michal, David Stillwell, and Thore Graepel. 2013. "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior." *Proceedings of the National Academy of Sciences* 110 (15): 5802–5. https://doi.org/10.1073/pnas.1218772110.

Koskenniemi, Martti. 2025. "The Laws That Rule Us." *New Left Review* 154 (August): 15–48.

Kosta, Eleni. 2020. "Article 35. Data Protection Impact Assessment." In *The EU General Data Protection Reuglation (GDPR): A Commentary*, 1st ed., edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Kotschy, Waltraut. 2020a. "Article 6. Lawfulness of Processing." In *The EU General Data Protection Reuglation (GDPR): A Commentary*, 1st ed., edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Kotschy, Waltraut. 2020b. "Article 79 Right to an Effective Judicial Remedy against a Controller or Processor." In *The EU General Data Protection Regulation (GDPR)*, edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University PressNew York. https://doi.org/10.1093/oso/9780198826491.003.0125.

Koukiadaki, Aristea. 2019. "Application (Article 51) and Limitations (Article 52(1))." In *The Charter of Fundamental Rights of the European Union and the Employment Relation*, edited by Filip Dorssemont. Hart.

Kountouris, Nicola. 2018. "The Concept of 'Worker' in European Labour Law: Fragmentation, Autonomy and Scope." *Industrial Law Journal* 47 (2): 192–225. https://doi.org/10.1093/indlaw/dwx014.

Kramcsák, Pablo Trigo. 2023. "Can Legitimate Interest Be an Appropriate Lawful Basis for Processing Artificial Intelligence Training Datasets?" *Computer Law & Security Review* 48 (April): 105765. https://doi.org/10.1016/j.clsr.2022.105765.

Kshetri, Nir. 2025. "Redefining Human Resource Practices With AI Agents and Agentic AI: Automated Compliance and Enhanced Productivity." *Computer* 58 (6): 119–24. https://doi.org/10.1109/MC.2025.3559245.

Kullmann, Miriam. 2019. "Discriminating Job Applicants Through Algorithmic Decision-Making." *Ars Aequi*, ahead of print. https://doi.org/10.2139/ssrn.3373533.

Kumar, Naveen. 2025. *AI Recruitment Statistics 2025 (Worldwide Data & Insights)*. Demandsage.com. June 23. (accessed 8.7.2025)

Kuner, Christopher, Lee A Bygrave, Christopher Docksey, and Laura Drechsler, eds. 2020. *The EU General Data Protection Reuglation (GDPR): A Commentary*. 1st ed. Oxford University Press.

Kuner, Christopher, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, and Christopher Millard. 2017. "Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?" *International Data Privacy Law* 7 (1): 1–2. https://doi.org/10.1093/idpl/ipx003.

Kuru, Taner. 2024. "Lawfulness of the Mass Processing of Publicly Accessible Online Data to Train Large Language Models." *International Data Privacy Law*, October 9, ipae013. https://doi.org/10.1093/idpl/ipae013.

Laat, Paul B. de. 2022. "Algorithmic Decision-Making Employing Profiling: Will Trade Secrecy Protection Render the Right to Explanation Toothless?" *Ethics and Information Technology* 24 (2): 17. https://doi.org/10.1007/s10676-022-09642-1.

Laato, Samuli, Teemu Birkstedt, Matti Mäantymäki, Matti Minkkinen, and Tommi Mikkonen. 2022. "AI Governance in the System Development Life Cycle: Insights on Responsible Machine Learning Engineering." *Proceedings of the 1st International Conference on AI Engineering: Software Engineering for AI* (New York, NY, USA), CAIN '22, October 17, 113–23. https://doi.org/10.1145/3522664.3528598.

Lacková, Eva. 2022. "Fragility of pre-contractual labour relations in the light of algorithmic recruitment." *Diritti Lavori Mercati International*, no. 2: 71–91.

Lafarre, Anne. 2023. "The Proposed Corporate Sustainability Due Diligence Directive: Corporate Liability Design for Social Harms." *European Business Law Review* 34 (Issue 2): 213–40. https://doi.org/10.54648/EULR2023017.

Lambrecht, Anja, and Catherine E. Tucker. 2019. "Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads." *Management Science* 65 (7). https://doi.org/https://doi.org/10.1287/mnsc.2018.3093.

Lanamäki, Arto, Mika Viljanen, Karin Väyrynen, and Lyria Bennett Moses. 2025. "Legal Compliance and the Open Texture of Law." *Journal of the Association for Information Systems* 26 (1): 1–8. https://doi.org/10.17705/1jais.00922.

Langer, Markus, Cornelius J. König, Diana Ruth-Pelipez Sanchez, and Sören Samadi. 2019. "Highly Automated Interviews: Applicant Reactions and the Organizational Context." *Journal of Managerial Psychology* 35 (4): 301–14. https://doi.org/10.1108/JMP-09-2018-0402.

Larsson, Stefan, James Merricks White, and Claire Ingram Bogusz. 2024. "The Artificial Recruiter: Risks of Discrimination in Employers' Use of AI and Automated Decision-Making." *Social Inclusion* 12 (0). https://doi.org/10.17645/si.7471.

Lasek-Markey, Marta, and Linda Hogan. 2025. "Delivering on the Promise of the Fundamental Rights Impact Assessments in the EU AI Act: Intersectionality and Vulnerability." *European Journal of Law and Technology* 16 (2). <https://www.ejlt.org/index.php/ejlt/article/view/1046>.

Lasser, Mitchel de S. -O. -L'E. 2004. *Judicial Deliberations - A Comparative Analysis of Judicial Transparency and Legitimacy.* 1st ed. Oxford Studies in European Law. Oxford University Press.

Latvian Data State Inspectorate. 2024. "Types of Processing Operations, for Which No Data Protection Impact Assessment Is Required in Accordance with Article 35(5) GDPR."

Lazcoz, Guillermo, and Paul de Hert. 2022. *Humans in the GDPR and AIA Governance of Automated and Algorithmic Systems. Essential Pre-Requisites against Abdicating Responsibilities*. Working Paper No. 32. Brussels Privacy Hub. Vrije Universiteit Brussel.

Lea, Andrew. 2024. “Why Is AI Hard to Define?” *ITNOW* 66 (1): 58–59. https://doi.org/10.1093/itnow/bwae028. (accessed 10.3.2024)

Legora.com. 2025. “Legora.” July. (accessed 8.7.2025)

Leicht-Deobald, Ulrich, Thorsten Busch, Christoph Schank, et al. 2019. “The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity.” *Journal of Business Ethics* 160 (2): 377–92. https://doi.org/10.1007/s10551-019-04204-w.

Leinarte, Emilija. 2024. “The Classification of High-Risk AI Systems Under the EU Artificial Intelligence Act.” *Journal of AI Law and Regulation* 1 (3): 262–80. https://doi.org/10.21552/aire/2024/3/4.

Lenaerts, Koen. 2012. “Exploring the Limits of the EU Charter of Fundamental Rights.” *European Constitutional Law Review* 8 (3): 375–403. https://doi.org/10.1017/S1574019612000260.

Lenaerts, Koen, and Jose A. Gutierrez-Fons. 2014. “To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice.” *Columbia Journal of European Law* 20 (2): 3–61.

Lenaerts, Koen, Kathleen Gutman, and Janek Tomasz Nowak. 2023. “Union Law and National Procedures and Remedies.” In *EU Procedural Law*, 2nd ed., by Koen Lenaerts, Kathleen Gutman, and Janek Tomasz Nowak. Oxford University PressOxford. https://doi.org/10.1093/oso/9780198833086.003.0004.

Lepinkäinen, Nea. 2024. “Algoritmiset haitat - Tekoälyn riskit ja sääntelyn haasteet kiihtyvässä yhteiskunnassa.” Doctoral dissertation, University of Turku.

Leskinen, Minni. 2022. “De lege ferenda -tutkimuksesta metodina ja tieteenä.” *Lakimies* 120 (7–8): 7–8.

Leufer, Daniel, and Fanny Hidvegi. 2023. “The Pitfalls of the European Union’s Risk-Based Approach to Digital Rulemaking.” *UCLA Law Review Discourse* 71: 156–75.

Levashina, Julia, Christopher J. Hartwell, Frederick P. Morgeson, and Michael A. Campion. 2014. “The Structured Employment Interview: Narrative and Quantitative Review of the Research Literature.” *Personnel Psychology* 67 (1): 241–93. https://doi.org/10.1111/peps.12052.

Li, Chuan. 2020. *OpenAI’s GPT-3 Language Model: A Technical Overview*. <https://lambdalabs.com/blog/demystifying-gpt-3>.

Li, Lan, Tina Lassiter, Joohee Oh, and Min Kyung Lee. 2021. “Algorithmic Hiring in Practice: Recruiter and HR Professional’s Perspectives on AI Use in Hiring.” *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (New York, NY, USA), AIES ’21, July 30, 166–76. https://doi.org/10.1145/3461702.3462531.

Lievens, Filip, and Derek Chapman. 2019. “Recruitment and Selection.” *The SAGE Handbook of Human Resource Management*, 123–50.

Linna, Tuula. 1987. “Ulosottorealisoinnista de lege ferenda.” Doctoral dissertation, University of Turku.

Lipton, Zachary C. 2018. “In Machine Learning, the Concept of Interpretability Is Both Important and Slippery.” *Machine Learning*.

Llama Team, AI @ Meta. 2024. *The Llama 3 Herd of Models*. Meta.

Lobel, Orly. 2024. “Automation Rights: How to Rationally Design Humans-Out-Of-The-Loop Law.” SSRN Scholarly Paper No. 4845805. Social Science Research Network, April 1. https://doi.org/10.2139/ssrn.4845805.

Luccioni, Alexandra Sasha, and Joseph D. Viviano. 2021. “What’s in the Box? A Preliminary Analysis of Undesirable Content in the Common Crawl Corpus.” arXiv:2105.02732. Preprint, arXiv, May 31. https://doi.org/10.48550/arXiv.2105.02732.

Lynskey, Orla. 2015. *The Foundations of EU Data Protection Law*. 1st ed. Oxford Studies in European Law. Oxford University Press.

Lynskey, Orla. 2020. "Article 8: The Right to Data Protection." In *The EU Charter of Fundamental Rights in the Member States*, edited by Michal Bobek and Jeremias Adams-Prassl. Hart Publishing. https://doi.org/10.5040/9781509940943.

Määttä, Tapio. 2016. "Metodinen pluralismi oikeustieteessä – Ympäristöoikeudellisen tutkimuksen suuntaukset ja menetelmät." In *Oikeustieteellinen opinnäyte - Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta*, edited by Tarmo Miettinen. Edita Publishing Oy. <www.edilex.fi/kirjat/16170>.

Macan, Therese. 2009. "The Employment Interview: A Review of Current Studies and Directions for Future Research." *Human Resource Management Review*, Employee Selection at the Beginning of the 21st Century, vol. 19 (3): 203–18. https://doi.org/10.1016/j.hrmr.2009.03.006.

Maduro, Miguel Poiares. 2008. "Interpreting European Law - Judicial Adjudication in a Context of Constitutional Pluralism." SSRN Scholarly Paper No. 1134503. Social Science Research Network, June 3. https://doi.org/10.2139/ssrn.1134503.

Mainka, Spencer M. 2019. "Algorithm-Based Recruiting Technology in the Workplace." *Texas A&M Journal of Property Law* 5 (3): 801–22.

Makkonen, Kaarle. 1981. *Oikeudellisen ratkaisutoiminnan ongelmia - Rakenneanalyyttinen tutkimus*. Suomalaisen Lakimiesyhdistyksen julkaisuja, B-sarja. Helsinki.

Malgieri, Gianclaudio. 2019. "Automated Decision-Making in the EU Member States: The Right to Explanation and Other 'Suitable Safeguards' in the National Legislations." *Computer Law & Security Review* 35: 1–26.

Malgieri, Gianclaudio. 2020. "The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation." *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, January 27, 154–66. https://doi.org/10.1145/3351095.3372868.

Malgieri, Gianclaudio. 2023. *Vulnerability and Data Protection Law*. OUP Oxford.

Malgieri, Gianclaudio, and Giovanni Comandé. 2017. "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation." *International Data Privacy Law* 7 (4): 243–65. https://doi.org/10.1093/idpl/ipx019.

Malgieri, Gianclaudio, and Cristiana Santos. 2025. "Assessing the (Severity of) Impacts on Fundamental Rights." *Computer Law & Security Review* 56 (April): 106113. https://doi.org/10.1016/j.clsr.2025.106113.

Mantelero, Alessandro. 2024. "The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template." *Computer Law & Security Review* 54 (September): 106020. https://doi.org/10.1016/j.clsr.2024.106020.

Marabelli, Marco, Sue Newell, and Valerie Handunge. 2021. "The Lifecycle of Algorithmic Decision-Making Systems: Organizational Choices and Ethical Challenges." *The Journal of Strategic Information Systems* 30 (3): 101683. https://doi.org/10.1016/j.jsis.2021.101683.

Martínez Ramil, Pablo. 2021. "Is the EU Human Rights Legal Framework Able to Cope with Discriminatory AI?" *IDP Revista de Internet Derecho y Política*, no. 34 (December): 1–14. https://doi.org/10.7238/idp.v0i34.387481.

Martínez-Ramil, Pablo. 2022. "Discriminatory Algorithms. A Proportionate Means of Achieving a Legitimate Aim?" *Journal of Ethics and Legal Technologies* 4 (1): 3–24.

Mast, Tobias, and Christian Ollig. 2023. "The Lazy Legislature: Incorporating and Horizontalising the Charter of Fundamental Rights through Secondary Union Law." *European Constitutional Law Review* 19 (3): 462–86. https://doi.org/10.1017/S1574019623000238.

Masterman, Tula, Sandi Besen, Mason Sawtell, and Alex Chao. 2024. “The Landscape of Emerging AI Agent Architectures for Reasoning, Planning, and Tool Calling: A Survey.” arXiv:2404.11584. Preprint, arXiv, April 17. <http://arxiv.org/abs/2404.11584>.

McCarthy, John, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon. 1955. *A Proposal For the Dartmouth Summer Research Project on Artificial Intelligence*. August 31.

McDonald, Aleecia M, and Lorrie Faith Cranor. 2008. “The Cost of Reading Privacy Policies.” *A Journal of Law and Policy for the Information Society* 4 (3): 543–68.

Mendoza, Isak, and Lee A Bygrave. 2017. “The Right Not to Be Subject to Automated Decisions Based on Profiling.” University of Oslo Faculty of Law Research Paper No. 2017-20. Preprint.

Menegatti, Emanuele. 2020. “Taking EU Labour Law beyond the Employment Contract: The Role Played by the European Court of Justice.” *European Labour Law Journal* 11 (1): 26–47. https://doi.org/10.1177/2031952519884713.

Meng, Qingxin, Keli Xiao, Dazhong Shen, Hengshu Zhu, and Hui Xiong. 2022. “Fine-Grained Job Salary Benchmarking with a Nonparametric Dirichlet Process–Based Latent Factor Model.” *INFORMS Journal on Computing* 34 (5): 2443–63. https://doi.org/10.1287/ijoc.2022.1182.

Menon, Vishnu M, and H. A. Rahulnath. 2016. “A Novel Approach to Evaluate and Rank Candidates in a Recruitment Process by Estimating Emotional Intelligence through Social Media Data.” 6.

Metaview. 2025. “Automatic, AI-Generated Interview Notes | Metaview.” <https://www.metaview.ai/>. (accessed 26.3.2025)

Metikoš, Ljubiša. 2025. “Dun & Bradstreet: A Pyrrhic Victory for the Contestation of AI under the GDPR.” Page. Faculteit Rechtsgeleerdheid En Criminologische Wetenschappen. <https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/dun-bradstreet-a-pyrrhic-victory-for-the-contestation-of-ai-under-the-gdpr>.

Metikoš, Ljubiša, and Jef Ausloos. 2025. “The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act.” *Law, Innovation and Technology* 17 (1): 205–40. https://doi.org/10.1080/17579961.2025.2469349.

Milanez, Anna, Annika Lemmens, and Carla Ruggiu. 2025. *Algorithmic Management in the Workplace - New Evidence From an OECD Employer Survey*. Paper No. 31. OECD Artificial Intelligence Papers. OECD.

Miller, Tim. 2019. “Explanation in Artificial Intelligence: Insights from the Social Sciences.” *Artificial Intelligence* 267 (February): 1–38. https://doi.org/10.1016/j.artint.2018.07.007.

Mitchell, Melanie. 2023. “How Do We Know How Smart AI Systems Are?” *Science* 381 (6654). https://doi.org/10.1126/science.adj5957.

Mittelstadt, Brent, Chris Russell, and Sandra Wachter. 2019. “Explaining Explanations in AI.” *Proceedings of the Conference on Fairness, Accountability, and Transparency*, January 29, 279–88. https://doi.org/10.1145/3287560.3287574.

Mittelstadt, Brent, Sandra Wachter, and Chris Russell. 2023. “To Protect Science, We Must Use LLMs as Zero-Shot Translators.” *Nature Human Behaviour* (London, United States) 7 (11): 1830–32. https://doi.org/10.1038/s41562-023-01744-0.

Molè, Michele. 2025. “Commodified, Outsourced Authority: A Research Agenda for Algorithmic Management at Work.” *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.5086055.

Moses, Lyria Bennett. 2007. “Recurring Dilemmas: The Law’s Race to Keep Up With Technological Change.” *University of Illinois Journal of Law, Technology & Policy*, no. 2: 239–86. https://doi.org/10.2139/ssrn.979861.

Moses, Lyria Bennett. 2013. “How to Think about Law, Regulation and Technology: Problems with Technology as a Regulatory Target.” *Law, Innovation and Technology* 5 (1): 1–20.

Muir, Elise. 2018. *EU Equality Law: The First Fundamental Rights Policy of the EU*. Oxford Studies in European Law. Oxford University Press.

Muir, Elise. 2019. “The Horizontal Effects of Charter Rights Given Expression to in EU Legislation, from Mangold to Bauer.” *Review of European Administrative Law* 12 (2): 185–215.

Muir, Elise, Mark Dawson, and Bruno de Witte. 2013. “1. Introduction: The European Court of Justice as a Political Actor.” In *Judicial Activism at the European Court of Justice*, edited by Mark Dawson, Bruno de Witte, and Muir Elise. Edward Elgar Publishing.

Neergaard, Ulla, and Ruth Nielsen. 2011. “Where Did the Spirits and Its Friends Go? On the European Legal Method(s) and the Interpretational Style of the Court of Justice of the European Union.” In *European Legal Method - Paradoxes and Revitalisation*, edited by Ulla Neergaard, Ruth Nielsen, and Lynn Roseberry. DJOF Publishing.

Nessler, Bernhard, and Christiane Wendehorst. 2024. “The Concept of ‘AI System’ under the New AI Act: Arguing for a Three-Factor Approach.” European Law Institute. <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf?utm_source=substack&utm_medium=email>.

Nielsen, Ruth. 2013. “New European Legal Realism - New Problems, New Solutions?” In *European Legal Method - towards a New European Legal Realism?*, edited by Ulla Neergaard and Ruth Nielsen. DJOF Publishing.

Nisbett, Richard E, and Timothy DeCamp Wilson. 1977. “Telling More Than We Can Know: Verbal Reports on Mental Processes.” *American Psychological Association* 84 (3): 231–59.

Nisevic, Maja, Arno Cuypers, and Jan De Bruyne. 2024. “Explainable AI: Can the AI Act and the GDPR Go out for a Date?” *2024 International Joint Conference on Neural Networks (IJCNN)*, June, 1–8. https://doi.org/10.1109/IJCNN60899.2024.10649994.

Nnawuchi, Uchenna, and Carlisle George. 2024. “A Grand Entrance Without a Blueprint: A Critical Analysis of the Right to Explanation in Article 86 of the European Union Artificial Intelligence Act.” *Journal of AI Law and Regulation* 1 (4): 402–19. https://doi.org/10.21552/aire/2024/4/6.

NotebookLM.google. 2025. “NotebookLM.” (accessed 8.7.2025)

Nouwens, Midas, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. “Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence.” *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, April 21, 1–13. https://doi.org/10.1145/3313831.3376321.

Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi. 2024. “Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity.” *Computer Law & Security Review*, October, 106066. https://doi.org/10.1016/j.clsr.2024.106066.

noyb. 2024. *ChatGPT Provides False Information about People, and OpenAI Can’t Correct It*. April 29. <https://noyb.eu/en/chatgpt-provides-false-information-about-people-and-openai-cant-correct-it>. (accessed 9.5.2025)

noyb. 2025. “Data Protection Day: Only 1.3% of Cases before EU DPAs Result in a Fine.” January 28. <https://noyb.eu/en/data-protection-day-only-13-cases-eu-dpas-result-fine>. (accessed 2.2.2026)

OECD. 2023. *AI Language Models: Technological, Socio-Economic and Policy Considerations*. OECD Digital Economy Papers No. 352. Vol. 352. OECD Digital Economy Papers. https://doi.org/10.1787/13d38f92-en.

OECD. 2024. "Recommendation of the Council on Artificial Intelligence - OECD/LEGAL/0449." OECD.

OECD. 2025. "AI Principles Overview." <https://oecd.ai/en/principles>.

Ogus, Anthony. 2004. *Regulation: Legal Form and Economic Theory*. Hart Publishing.

Ohm, Paul. 2024. "Focusing on Fine-Tuning: Understanding the Four Pathways for Shaping Generative AI." SSRN Scholarly Paper No. 4738261. Social Science Research Network, June 21. https://doi.org/10.2139/ssrn.4738261.

Ojanen, Atte, Otto Sahlgren, Juho Vaiste, et al. 2022. *Algoritminen syrjintä ja yhdenvertaisuuden edistäminen : Arviointikehikko syrjimättömälle tekoälylle*.

Oleeo. 2025. "ATS Recruitment Software - Identify & Track Your Top Talent." Oleeo. <https://www.oleeo.com/products/ats-software/>. (accessed 26.3.2025)

Oliver, Nuria, and Rishi Bommasani. 2025. "Code of Practice for General-Purpose AI Models - Transparency Chapter."

O'Meara, Bernard, and Stanley Petzall. 2013. *The Handbook of Strategic Recruitment and Selection : A Systems Approach*. 1st ed. Bingley, United Kingdom : Emerald.

OpenAI. 2023a. "GPT-4 System Card." March 23. <https://cdn.openai.com/papers/gpt-4-system-card.pdf>.

OpenAI. 2023b. "GPT-4 Technical Report." arXiv:2303.08774. Preprint, arXiv, March 27. <http://arxiv.org/abs/2303.08774>.

OpenAI. 2025a. *1 Million Business Customers: The Fastest-Growing Business Platform in History*. Openai.com. May 11.

OpenAI. 2025b. "Usage Policies - OpenAI." OpenAI, January 29. <https://openai.com/en-GB/policies/usage-policies/>.

Ore, Olajide, and Martin Sposato. 2022. "Opportunities and Risks of Artificial Intelligence in Recruitment and Selection." *International Journal of Organizational Analysis* 30 (6): 1771–82. https://doi.org/10.1108/IJOA-07-2020-2291.

Orlitzky, Marc. 2009. *Recruitment Strategy*. Edited by Peter Boxall, John Purcell, and Patrick M. Wright. Vol. 1. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199547029.003.0014.

Otto, Marta. 2018. "Workforce Analytics v Fundamental Rights Protection in the EU in the Age of Big Data." *Comparative Labor Law & Policy Journal* 40 (3): 389–404.

Palmiotto, Francesca. 2024. "When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis." *German Law Journal* 25 (2): 210–36. https://doi.org/10.1017/glj.2023.112.

Parodi, Elisa. 2024. "Discrimination in the Automated Targeting of Job Advertising: The Role of the General Data Protection Regulation." *European Labour Law Journal*, October 13, 109–22. https://doi.org/10.1177/20319525241285424.

Parviainen, Henni. 2020. "Automated Decision-Making and Profiling in Recruitment - an Impossible Equation from Data Protection and Employment Law Perspective?" Master's Thesis, Aalto University.

Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Passi, Samir, and Solon Barocas. 2019. "Problem Formulation and Fairness." *Proceedings of the Conference on Fairness, Accountability, and Transparency* (New York, NY, USA), FAT* '19, January 29, 39–48. https://doi.org/10.1145/3287560.3287567.

Pathak, Gangesh, and Divya Pandey. 2025. “AI Agents in Recruitment: A Multi-Agent System for Interview, Evaluation, and Candidate Scoring.” SSRN Scholarly Paper No. 5242372. Social Science Research Network, May 1. https://doi.org/10.2139/ssrn.5242372.

Patil, Avinash. 2025. “Advancing Reasoning in Large Language Models: Promising Methods and Approaches.” arXiv:2502.03671. Preprint, arXiv, May 28. <http://arxiv.org/abs/2502.03671>.

Paunio, Elina. 2011. “Beyond Words - The European Court of Justice and Legal Certainty in Multilingual EU Law.” University of Helsinki.

Peck, Don. 2013. “They’re Watching You at Work.” *The Atlantic*, December. <https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/>. (accessed 12.11.2025)

Peczenik, Aleksander. 1983. “The Basis of Legal Justification.” Doctoral Dissertation, Lund University.

Peukert, Alexander, and Céline Castets-Renard. 2025. “Code of Practice for General-Purpose AI Models - Copyright Chapter.”

Prahl, Andrew, and Lyn Van Swol. 2017. “Understanding Algorithm Aversion: When Is Advice from Automation Discounted?” *Journal of Forecasting* 36 (6): 691–702. https://doi.org/10.1002/for.2464.

Prassl, Jeremias. 2015. *The Concept of the Employer*. Oxford University Press.

Prince, Anya E R, and Daniel Schwarcz. 2020. “Proxy Discrimination in the Age of Artificial Intelligence and Big Data.” *Iowa Law Review* 105 (3): 1257–318.

Publication I / Viljanen, Mika, and Henni Parviainen. 2022. “AI Applications and Regulation: Mapping the Regulatory Strata.” *Frontiers in Computer Science* 3. <https://www.frontiersin.org/article/10.3389/fcomp.2021.779957>.

Publication II /Parviainen, Henni. 2022. “Can Algorithmic Recruitment Systems Lawfully Utilise Automated Decision-Making in the EU?” *European Labour Law Journal* 13 (2): 225–48. https://doi.org/10.1177/20319525221093815.

Publication III / Parviainen, Henni. 2024. “Challenges of Direct Discrimination in Algorithmic Recruitment: Insuperable or Not?*.” *International Journal of Comparative Labour Law and Industrial Relations* 40 (Issue 4): 437–66. https://doi.org/10.54648/IJCL2024017.

Publication IV / Parviainen, Henni. 2026. “Effective Remedies for Job Applicants in Algorithmic Recruitment: The Contribution of the EU Artificial Intelligence Act.” *Accepted for Publication in Law, Innovation and Technology*.

Purtova, Nadezhda. 2018. “The Law of Everything. Broad Concept of Personal Data.” *Law, Innovation and Technology* 10 (1): 40–81. https://doi.org/10.1080/17579961.2018.1452176.

pymetrics. 2023. “Talent Management & Talent Acquisition Solutions Pymetrics.” <https://www.pymetrics.ai/talent-acquisition>. (accessed 26.3.2025)

Raghavan, Manish, Solon Barocas, Jon Kleinberg, and Karen Levy. 2019. “Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices.” *arXiv:1906.09208 [Cs]*, ahead of print, December 6. https://doi.org/10.1145/3351095.3372828.

Raitio, Juha. 2013. “The Expectation of Legal Certainty and Horizontal Effect of EU Law.” In *General Principles of EU Law and European Private Law*. European Monographs 84. Kluwer Law International BV.

Raso, Filippo, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, and Levin Kim. 2018. “Artificial Intelligence & Human Rights- Opportunities and Risks.” Berkman Klein Center for internet & society at Harvard University.

Rathnayake, Chaminda, and Aruni Gunawardana. 2023. “The Role of Generative AI in Enhancing Human Resource Management Recruitment, Training, and Performance Evaluation Perspectives.” *International Journal of Social Analytics* 8 (11): 11.

Rautiainen, Pauli, Kostiainen Aura, Visa Kurki, Niko Soininen, and Tapio Määttä. 2023. *Oikeus ja sen tutkiminen*. Vastapaino.

Rebrean, Maria-Lucia, and Gianclaudio Malgieri. 2025. “Vulnerability in the EU AI Act: Building an Interpretation.” *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, June 23, 1985–97. https://doi.org/10.1145/3715275.3732133.

Registry of the European Court of Human Rights. 2025. *Guide on Article 14 of the Convention (Prohibition of Discrimination) and on Article 1 of Protocol No. 12 to the Convention - Prohibition of Discrimination.* Case-Law Guide.

ResearchRabbit.ai. 2025. “ResearchRabbit.” <https://www.researchrabbit.ai/>. (accessed 23.4.2025)

Reynolds, Douglas H., and David N. Dickter. 2017. “Technology and Employee Selection.” In *Handbook of Employee Selection*, 2nd ed., edited by James L. Farr, Nancy T. Tippins, Walter C. Borman, et al. Routledge. https://doi.org/10.4324/9781315690193-39.

Riede, Lutz, and Oliver Talhoff. 2024. “Article 25 - Responsibilities Along the AI Value Chain.” In *The EU Artificial Intelligence (AI) Act : A Commentary*, edited by Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. Kluwer Law International.

Rigotti, Carlotta, and Eduard Fosch-Villaronga. 2024. “Fairness, AI & Recruitment.” *Computer Law & Security Review* 53 (July): 105966. https://doi.org/10.1016/j.clsr.2024.105966.

Risse, Mathias. 2019. “Human Rights and Artificial Intelligence: An Urgently Needed Agenda.” *Human Rights Quarterly* 41 (1): 1–16. 134595375. https://doi.org/10.1353/hrq.2019.0000.

Robbins, Bruce. 2024. “RAG in Recruitment in AI-Powered Recruitment.” *Medium*, September 2. <https://medium.com/@brucerobbins/rag-in-recruitment-7c15d6d24b20>. (accessed 9.12.2024)

Rodrigues, Carlos. 2024. *Generative AI Foundations in Python: Discover Key Techniques and Navigate Modern Challenges in LLMs*. Packt Publishing.

Root, Veronica. 2019. “The Compliance Process.” *Indiana Law Journal* 94.

Rosin, Annika, and Henni Parviainen. 2025. “Improving the Transparency of Algorithmic Management in Platform Work: The Role of the Platform Work Directive.” *European Labour Law Journal*, ahead of print, September 10. https://doi.org/10.1177/20319525251375023.

Salesforce Research. 2025. “HR Leaders to Redeploy a Quarter of Their Workforce as Agentic AI Adoption Expected to Grow 327% by 2027.” *Salesforce*, May 5. <https://www.salesforce.com/news/stories/agentic-ai-impact-on-workforce-research/>. (accessed 24.6.2025)

Samwald, Matthias, Yoshua Bengio, Marietje Schaake, et al. 2025. “Code of Practice for General-Purpose AI Models - Safety and Security Chapter.”

Sánchez-Monedero, Javier, Lina Dencik, and Lilian Edwards. 2020. “What Does It Mean to Solve the Problem of Discrimination in Hiring? Social, Technical and Legal Perspectives from the UK on Automated Hiring Systems.” *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Barcelona Spain), January 17, 458–68. https://doi.org/https://doi.org/10.1145/3351095.3372849.

Sapia.ai. 2025. “Sapia.Ai Home 2025.” Sapia.Ai. <https://sapia.ai/>. (accessed 26.3.2025)

Sartor, Giovanni, and Francesca Lagioia. 2020. *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*. EPRS European Parliamentary Research Service. <http://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf>.

Schadewijk, Matthijs van. 2021. “The Notion of ‘Employer’: Towards a Uniform European Concept?” *European Labour Law Journal*, February 11, 363–86. https://doi.org/10.1177/2031952521991159.

Schearer, Colin. 2000. *CRISP-DM The New Blueprint for Data Mining*. <https://www.academia.edu/42079490/CRISP_DM_The_New_Blueprint_for_Data_Mining_Colin_Shearer_Fall_2000_>.

Scherer, Matthew U. 2016. “Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies.” *Harvard Journal of Law & Technology* 29 (2): 353–400. https://doi.org/10.2139/ssrn.2609777.

Schermers, Henry G., and Denis F. Waelbroeck. 2001. *Judicial Protection in the European Union*. 6th ed. Kluwer Law International.

Schlag, Pierre. 2007. “Spam Jurisprudence, Air Law, and the Rank Anxiety of Nothing Happening (a Report on the State of the Art).” *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.976078.

Schønberg, Sören, and Karin Frick. 2003. “Finishing, Refining, Polishing: On the Use of Travaux Preparatoires as an Aid to the Interpretation of Community Legislation.” *European Law Review* 28 (2): 149–71.

Schuett, Jonas. 2019. “A Legal Definition of AI.” *arXiv:1909.01095 [Cs]*, August 26. <http://arxiv.org/abs/1909.01095>.

Schuett, Jonas. 2023. “Defining the Scope of AI Regulations.” *Law, Innovation and Technology* 0 (0): 1–23. https://doi.org/10.1080/17579961.2023.2184135.

Scispace.com. 2025. “AI-Powered Data Extraction from Research PDFs | SciSpace.” <https://scispace.com/extract-data>. (accessed 24.4.2025)

Scite.ai. 2025. “AI for Research | Scite.” <https://scite.ai/home>. (accessed 24.4.2025)

Sen, Sujoy, Sanjeev Kadam, and V.V. Ravi Kumar. 2023. “Role of Artificial Intelligence-Enabled Recruitment Processes in Sourcing Talent.” *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, March, 1–5. https://doi.org/10.1109/ISCON57294.2023.10112009.

Sevilla, Jaime, Lennart Heim, Anson Ho, Tamay Besiroglu, Marius Hobbhahn, and Pablo Villalobos. 2022. “Compute Trends Across Three Eras of Machine Learning.” arXiv:2202.05924. Preprint, arXiv, March 9. https://doi.org/10.48550/arXiv.2202.05924.

Sharma, Siddharth. 2024. “Addressing Deepfake Challenges In The Hiring Landscape.” *Forbes*, February 16. <https://www.forbes.com/councils/forbeshumanresourcescouncil/2024/02/16/addressing-deepfake-challenges-in-the-hiring-landscape/>. (accessed 17.9.2025)

Shavell, Steven. 1993. “The Optimal Structure of Law Enforcement.” *Journal of Law & Economics* 36 (1): 255–88.

Siltala, Raimo. 2003. *Oikeustieteen Tieteenteoria*. Suomalainen Lakimiesyhdistys. Vammala.

Silva, Daswin De, and Damminda Alahakoon. 2022. “An Artificial Intelligence Life Cycle: From Conception to Production.” *Patterns* 3 (6). https://doi.org/10.1016/j.patter.2022.100489.

Sison, Alejo José G., Marco Tulio Daza, Roberto Gozalo-Brizuela, and Eduardo C. Garrido-Merchán. 2024. “ChatGPT: More Than a ‘Weapon of Mass Deception’ Ethical Challenges and Responses from the Human-Centered Artificial Intelligence (HCAI) Perspective.” *International Journal of Human–Computer Interaction* 40 (17): 4853–72. https://doi.org/10.1080/10447318.2023.2225931.

Sivathanu, Brijesh, and Rajasshrie Pillai. 2019. "Technology and Talent Analytics for Talent Management – a Game Changer for Organizational Performance." *International Journal of Organizational Analysis* 28 (2): 457–73. https://doi.org/10.1108/IJOA-01-2019-1634.

Skitka, Linda J., Kathleen Mosier, and Mark D. Burdick. 2000. "Accountability and Automation Bias." *International Journal of Human-Computer Studies* 52 (4): 701–17. https://doi.org/10.1006/ijhc.1999.0349.

Skitka, Linda J., Kathleen L. Mosier, and Mark Burdick. 1999. "Does Automation Bias Decision-Making?" *International Journal of Human-Computer Studies* 51 (5): 991–1006. https://doi.org/10.1006/ijhc.1999.0252.

Sloot, Bart van der. 2016. "The Practical and Theoretical Problems with 'Balancing': Delfi, Coty and the Redundancy of the Human Rights Framework." *Maastricht Journal of European and Comparative Law* 23 (3): 439–59. https://doi.org/10.1177/1023263X1602300304.

Smith, Andrew L., Felix Greaves, and Trishan Panch. 2023. "Hallucination or Confabulation? Neuroanatomy as Metaphor in Large Language Models." *PLOS Digital Health* 2 (11): e0000388. https://doi.org/10.1371/journal.pdig.0000388.

Smits, Jan M. 2017. "What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research." In *Rethinking Legal Scholarship : A Transatlantic Dialogue*, edited by Rob van Gestel, Hans-Wolfgang Micklitz, and Edwards L. Rubin.

Smuha, Nathalie A. 2021. "From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence." *Law, Innovation and Technology* 13 (1): 57–84. https://doi.org/10.1080/17579961.2021.1898300.

Smuha, Nathalie A. 2024a. *Algorithmic Rule By Law: How Algorithmic Regulation in the Public Sector Erodes the Rule of Law*. 1st ed. Cambridge University Press. https://doi.org/10.1017/9781009427500.

Smuha, Nathalie A. 2024b. *The Paramountcy of Data Protection Law in the Age of AI (Acts)*. Two decades of personal data protection. What next? EDPS 20th Anniversary. European Data Protection Supervisor.

Smuha, Nathalie A., and Karen Yeung. 2025. "The European Union's AI Act: Beyond Motherhood and Apple Pie?" In *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, edited by Nathalie A. Smuha. Cambridge Law Handbooks. Cambridge University Press. https://doi.org/10.1017/9781009367783.015.

SocialFinder.ai. 2025. "SocialFinder.Ai." SocialFinder.Ai. <https://socialfinder.ai>. (accessed 25.3.3025)

Söllner, Matthias, Thomas Arnold, Alexander Benlian, et al. 2025. "ChatGPT and Beyond: Exploring the Responsible Use of Generative AI in the Workplace." *Business & Information Systems Engineering*, ahead of print, February 12. https://doi.org/10.1007/s12599-025-00932-8.

Solove, Daniel J. 2013. "Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126: 1880–903.

Solove, Daniel J., and Woodrow Hartzog. 2024. "The Great Scrape: The Clash Between Scraping and Privacy." SSRN Scholarly Paper No. 4884485. Rochester, NY, July 3. https://doi.org/10.2139/ssrn.4884485.

Srinivasan, Hari. 2024. "Reimagining Hiring and Learning With the Power of AI." Linkedin. *LinkedIn Talent Blog*. <https://www.linkedin.com/business/talent/blog/talent-acquisition/reimagining-hiring-and-learning-with-power-of-ai>. (accessed 21.11.2024)

Stone, Dianna L., Kimberly M. Lukaszewski, Eugene F. Stone-Romero, and Teresa L. Johnson. 2013. "Factors Affecting the Effectiveness and Acceptance of Electronic Selection Systems."

Human Resource Management Review 23 (1): 50–70. https://doi.org/10.1016/j.hrmr.2012.06.006.

Stryker, Cole. 2025. "What Is Agentic AI? | IBM." February 24. <https://www.ibm.com/think/topics/agentic-ai>. (accessed 24.6.2025)

Suen, Hung-Yue. 2018. "How Passive Job Candidates Respond to Social Networking Site Screening." *Computers in Human Behavior* 85 (August): 396–404. https://doi.org/10.1016/j.chb.2018.04.018.

Suksi, Markku. 2020. "Administrative Due Process When Using Automated Decision-Making in Public Administration: Some Notes from a Finnish Perspective." *Artificial Intelligence and Law*, ahead of print, May 22. https://doi.org/10.1007/s10506-020-09269-x.

Tecqmenne, Maxime. 2024. "The European Court of Justice, the EU Charter and the Interpretation of Fundamental Social Rights: Judicial Law-Making in Disguise?" *Maastricht Journal of European and Comparative Law* 31 (2): 254–72. https://doi.org/10.1177/1023263X241288909.

Teo, Sue Anne. 2023. "Towards Human Rights 2.0?: A Meta-Theoretical Analysis of the Disruptions to Human Rights Foundations by Artificial Intelligence." Doctoral Thesis (compilation).

Terwangne, Cécile de. 2020. "Article 5. Principles Relating to Processing of Personal Data." In *The EU General Data Protection Reuglation (GDPR): A Commentary*, 1st ed., edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Textio. 2023. "Textio – Interrupt Bias in Performance Feedback and Recruiting." <https://textio.com/>. (accessed 26.3.2025)

The Economist (Online). 2013. "How Might Your Choice of Browser Affect Your Job Prospects?" *The Economist (Online)* (London), October 4. <https://www.economist.com/the-economist-explains/2013/04/10/how-might-your-choice-of-browser-affect-your-job-prospects>.

The Office for Personal Data Protection Czech Republic. 2020. "List of Processing Operations for Which No DPIA Is Required (GDPR Article 35(5) List)."

Thomaidou, Anna, and Konstantinos Limniotis. 2025. "Navigating Through Human Rights in AI: Exploring the Interplay Between GDPR and Fundamental Rights Impact Assessment." *Journal of Cybersecurity and Privacy* 5 (1): 1. https://doi.org/10.3390/jcp5010007.

Tilmes, Nicholas. 2022. "Disability, Fairness, and Algorithmic Bias in AI Recruitment." *Ethics and Information Technology* 24 (2): 21. https://doi.org/10.1007/s10676-022-09633-2.

Tippins, Nancy, Frederick Oswald, and S. Morton McPhail. 2021. "Scientific, Legal, and Ethical Concerns About AI-Based Personnel Selection Tools: A Call to Action." *Personnel Assessment and Decisions* 7 (2). https://doi.org/10.25035/pad.2021.02.001.

Tobler, Christa. 2022. *Indirect Discrimination under Directives 2000/43 and 2000/78.* European Commission. Publications Office.

Tridimas, Takis. 2013. "Horizontal Effect of General Principles: Bold Rulings and Fine Distinctions." In *General Principles of EU Law and European Private Law*. European Monographs 84. Kluwer Law International BV.

Tridimas, Takis. 2014. "Fundamental Rights, General Principles of EU Law, and the Charter." *Cambridge Yearbook of European Legal Studies* 16: 361–92. https://doi.org/10.1017/S1528887000002676.

Tsakyrakis, S. 2009. "Proportionality: An Assault on Human Rights?" *International Journal of Constitutional Law* 7 (3): 468–93. https://doi.org/10.1093/icon/mop011.

Tuori, Kaarlo. 2011. *Ratio and Voluntas - The Tension Between Reason and Will in Law*. Applied Legal Philosophy. Ashgate Publishing Limited.

Tuori, Kaarlo. 2017. “The Pluralism of European Fundamental Rights Law.” In *Research Handbook on EU Law and Human Rights*, edited by Sionaidh Douglas-Scott and Nicholas Hatzis. Edward Elgar Publishing. https://doi.org/10.4337/9781782546405.00011.

Tutt, Andrew. 2016. “An FDA for Algorithms.” *Administrative Law Review* 69 (1): 83–123. https://doi.org/10.2139/ssrn.2747994.

UK National Cyber Security Centre, and US Cybersecurity and Infrastructure Security Agency. 2023. *Guidelines for Secure AI System Development*.

UNLEASH. 2023. *93% of HR Managers Use AI Tools to Reduce Costs, Report Finds*. December 15. <https://www.unleash.ai/artificial-intelligence/93-of-hr-managers-use-ai-tools-to-reduce-costs-report-finds/>. (accessed 24.11.2024)

U.S. Equal Employment Opportunity Commission. 2022. “The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees.” <https://perma.cc/LG25-D53T>.

Vale, Daniel, Ali El-Sharif, and Muhammed Ali. 2022. “Explainable Artificial Intelligence (XAI) Post-Hoc Explainability Methods: Risks and Limitations in Non-Discrimination Law.” *AI and Ethics*, ahead of print, March 15. https://doi.org/10.1007/s43681-022-00142-y.

Van Alsenoy, Brendan. 2016. “Liability under EU Data Protection Law.” *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 7 (3): 271–88.

Vaswani, Ashish, Noam Shazeer, Niki Parmar, et al. 2017. “Attention Is All You Need.” arXiv:1706.03762. Preprint, arXiv. https://doi.org/10.48550/arXiv.1706.03762.

Veale, Michael, Reuben Binns, and Lilian Edwards. 2018. “Algorithms That Remember: Model Inversion Attacks and Data Protection Law.” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376 (2133): 20180083. https://doi.org/10.1098/rsta.2018.0083.

Veale, Michael, and Frederik Zuiderveen Borgesius. 2021. *Demystifying the Draft EU Artificial Intelligence Act*. Preprint. SocArXiv. https://doi.org/10.31235/osf.io/38p5f.

Vedder, Anton, and Laurens Naudts. 2017. “Accountability for the Use of Algorithms in a Big Data Environment.” *International Review of Law, Computers & Technology* 31 (2): 206–24. https://doi.org/10.1080/13600869.2017.1298547.

Viljanen, Mika. 2022. “Technology Matters: How Algorithm and Artificial Intelligent Technology Features Affect Harms Reduction Efforts.” *Justice, Power and Resistance* 5 (3): 314–21. https://doi.org/10.1332/XFHZ3158.

Viljanen, Mika. 2023. “Menikö juna jo? Tekoälyn sääntelemisen mahdollisuuksista.” *Lakimies* 121 (7–8): 7–8.

Viljanen, Mika. 2024. “A Horizontal Meta-Effect? Theorising Human Rights in the AI Act and the Corporate Sustainability Due Diligence Directive.” In *YSEC Yearbook of Socio-Economic Constitutions 2023*, edited by Eduardo Gill-Pedro and Andreas Moberg, vol. 2023. YSEC Yearbook of Socio-Economic Constitutions. Springer Nature Switzerland. https://doi.org/10.1007/16495_2023_65.

Villaronga, Eduard Fosch, Peter Kieseberg, and Tiffany Li. 2018. “Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten.” *Computer Law & Security Review* 34 (2): 304–13. https://doi.org/10.1016/j.clsr.2017.08.007.

Voigt, Paul, and Nils Hullen. 2024. *The EU AI Act: Answers to Frequently Asked Questions*. 1st ed. Springer Berlin / Heidelberg.

Wachter, Sandra. 2022. “The Theory of Artificial Immutability: Protecting Algorithmic Groups under Anti-Discrimination Law.” *Tulane Law Review* 97 (2): 149–204.

Wachter, Sandra. 2024. “Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond.” *Yale Journal of Law & Technology* 26 (3): 671–718. https://doi.org/10.2139/ssrn.4924553.

Wachter, Sandra, and Brent Mittelstadt. 2019. “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI.” *Columbia Business Law Review*, no. 2: 494–620. https://doi.org/10.31228/osf.io/mu2kf.

Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. 2017. “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation.” *International Data Privacy Law* 7 (2): 76–99. https://doi.org/doi:10.1093/idpl/ipx005.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2018. “Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR.” *Harvard Journal of Law & Technology* 31 (2). https://doi.org/10.2139/ssrn.3063289.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2020. “Bias Preservation in Machine Learning: The Legality of Fairness Metrics under EU Non-Discrimination Law.” *West Virginia Law Review* 123 (3): 735–90.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2021. “Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI.” *Computer Law & Security Review* 41 (July): 105567. https://doi.org/10.1016/j.clsr.2021.105567.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. 2024. “Do Large Language Models Have a Legal Duty to Tell the Truth?” *Royal Society Open Science* 11 (8): 240197. https://doi.org/10.1098/rsos.240197.

Walker, Dayna O. H., and Milan Larson. 2025. “Leveraging Generative Artificial Intelligence (AI) for Human Resource Management: The AI Job Description Assignment.” *Journal of Management Education* 49 (1): 113–41. https://doi.org/10.1177/10525629241294075.

Walkila, Sonya. 2015. “Horizontal Effect of Fundamental Rights - Contributing to the ‘Primacy, Unity and Effectiveness of European Union Law.’” University of Helsinki.

Wang, Pei. 2019. “On Defining Artificial Intelligence.” *Journal of Artificial General Intelligence* 10 (2): 1–37. https://doi.org/10.2478/jagi-2019-0002.

Ward, Jonathan Stuart, and Adam Barker. 2013. “Undefined By Data: A Survey of Big Data Definitions.” arXiv:1309.5821. Preprint, arXiv, September 20. https://doi.org/10.48550/arXiv.1309.5821.

Warter, Johannes. 2025. “The Legitimacy of Modern Data Processing in the Workplace.” *European Labour Law Journal* 16 (2): 179–94. https://doi.org/10.1177/20319525251332923.

Watson, Nell. 2025. “The Challenges of Agentic AI Safety.” In *The Oxford Handbook of the Foundations and Regulation of Generative AI*, edited by Philipp Hacker, Brent Daniel Mittelstadt, Sarah Hammer, and Andreas Engel. Oxford University Press.

Weerts, Hilde, Aislinn Kelly-Lyth, Reuben Binns, and Jeremias Adams-Prassl. 2024. “Unlawful Proxy Discrimination: A Framework for Challenging Inherently Discriminatory Algorithms.” *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, June 3, 1850–60. https://doi.org/10.1145/3630106.3659010.

Wei, Jason, Xuezhi Wang, Dale Schuurmans, et al. 2023. “Chain-of-Thought Prompting Elicits Reasoning in Large Language Models.” arXiv:2201.11903. Preprint, arXiv, January 10. https://doi.org/10.48550/arXiv.2201.11903.

Weidinger, Laura, Jonathan Uesato, Maribeth Rauh, et al. 2022. “Taxonomy of Risks Posed by Language Models.” *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA), FAccT ’22, June 20, 214–29. https://doi.org/10.1145/3531146.3533088.

Weilert, J H H. 1991. “The Transformation of Europe.” *Yale Law Journal* 100 (8).

Weiss, Manfred. 2011. “Re-Inventing Labour Law?” In *The Idea of Labour Law*, edited by Guy Davidov and Brian Langille. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199693610.003.0004.

Wiggers, Kyle. 2024. “Supervised vs. Unsupervised Learning: What’s the Difference?” IBM, April 24. <https://www.ibm.com/think/topics/supervised-vs-unsupervised-learning>. (accessed 20.12.2024)

Williams, Betsy Anne, Catherine F. Brooks, and Yotam Shmargad. 2018. “How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications.” *Journal of Information Policy* 8: 78–115. https://doi.org/10.5325/jinfopoli.8.2018.0078.

Williams, Paul R, Scott R Lyons, and Tali Neuwirth. 2004. “Preemption in the 21st Century: What Are the Legal Parameters?” *ILSA Journal of International & Comparative Law* 10 (2): 353–66.

Williams, Penny, Paula McDonald, and Robyn Mayes. 2021. “Recruitment in the Gig Economy: Attraction and Selection on Digital Platforms.” *The International Journal of Human Resource Management* 32 (19): 4136–62. https://doi.org/10.1080/09585192.2020.1867613.

Witte, Bruno de. 2011. “Direct Effect, Primacy, and the Nature of the Legal Order.” In *The Evolution of EU Law*, 2nd ed. Oxford University Press.

Witty.works. 2025. “Witty: Scale Inclusion Faster. With Language.” <https://www.witty.works>. (accessed 25.3.2025)

WP29. 2013. “Opinion 03/2013 on Purpose Limitation.” Article 29 Data Protection Working Party, February 4.

WP29. 2014. “Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC.” Article 29 Data Protection Working Party, September 4.

WP29. 2016. “Guidelines on the Right to Data Portability.” Article 29 Data Protection Working Party, December 13.

WP29. 2017a. “Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is ‘Likely to Result in a High Risk’ for the Purposes of Regulation 2016/679.” Article 29 Data Protection Working Party, April 10.

WP29. 2017b. “Opinion 2/2017 on Data Processing at Work (WP 249).” Article 29 Data Protection Working Party, August 6.

WP29. 2018a. “Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, Adopted on 3 October 2017, as Last Revised and Adopted on 6 February 2018, (WP251rev.01).” Article 29 Data Protection Working Party, June 2. <https://ec.europa.eu/newsroom/article29/items/612053>.

WP29. 2018b. “Guidelines on Consent under Regulation 2016/679.” Article 29 Data Protection Working Party, October 4.

WP29. 2018c. “Guidelines on Transparency under Regulation 2016/679.” Article 29 Data Protection Working Party, November 4.

Wu, Xuansheng, Haiyan Zhao, Yaochen Zhu, et al. 2024. “Usable XAI: 10 Strategies Towards Exploiting Explainability in the LLM Era.” arXiv:2403.08946. Preprint, arXiv, March 13. https://doi.org/10.48550/arXiv.2403.08946.

Xenidis, Raphaële, and Linda Senden. 2020. “EU Non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination.” In *General Principles of EU Law and the EU Digital Order*, edited by Ulf Bernitz, Xavier Groussot, Jaan Paju, and Sybe A. de Vries, vol. 12. European Monographs Series Set. Kluwer Law International BV.

Yeung, Karen. 2018. *A Study of the Implications of Advanced Digital Technologies (Including AI Systems) for the Concept of Responsibility within a Human Rights Framework.*

Yin, Leon, Davey Alba, and Leonardo Nicoletti. 2024. “OpenAI’s GPT Is a Recruiter’s Dream Tool - Tests Show There’s Racial Bias.” Bloomberg.

Yusifli, Zahra. 2024. “European Union · The ‘Bouncing Ball’ Effect of the EU Artificial Intelligence Act on Employment Relations.” *Journal of AI Law and Regulation* 1 (2): 228–32. https://doi.org/10.21552/aire/2024/2/9.

Zanfir-Fortuna, Gabriela. 2020. “Article 82 Right to Compensation and Liability.” In *The EU General Data Protection Reuglation (GDPR): A Commentary*, 1st ed., edited by Christopher Kuner, Lee A Bygrave, Christopher Docksey, and Laura Drechsler. Oxford University Press.

Zarsky, Tal Z. 2017. “Incompatible: The GDPR in the Age of Big Data.” *Seton Hall Law Review* 47: 995–1020.

Žliobaitė, Indrė, and Bart Custers. 2016. “Using Sensitive Personal Data May Be Necessary for Avoiding Discrimination in Data-Driven Decision Models.” *Artificial Intelligence and Law* 24 (2): 183–201. https://doi.org/10.1007/s10506-016-9182-5.

Zoho Recruit. 2025. “Recruiting Automation for Your Faster Hiring Needs - Zoho Recruit.” Zoho. <https://www.zoho.com/recruit/recruitment-automation.html>. (accessed 26.3.2025)

Zollo, Thomas P., Nikita Rajaneesh, Richard Zemel, Talia B. Gillis, and Emily Black. 2024. “Towards Effective Discrimination Testing for Generative AI.” arXiv:2412.21052. Preprint, arXiv, December 30. https://doi.org/10.48550/arXiv.2412.21052.

Zuboff, Shoshana. 2019. *Surveillance Capitalism - The Fight For a Human Future At The New Frontier Of Power*. Profile Books, London.

Case law

Court of Justice of the European Union

C-26/62 *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration,* 5.2.1963, ECLI:EU:C:1963:1.
C-6/64 *Flaminio Costa v ENEL (Ente Nazionale Energia Elettrica), 15.7.1964,* ECLI:EU:C:1964:66.
C-29/69 *Erich Stauder v City of Ulm, Sozialamt,* 12.11.1969, ECLI:EU:C:1969:57.
C-11/70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel,* 17.12.1970, ECLI:EU:C:1970:114.
C-41/74 *Yvonne van Duyn v Home Office,* 4.12.1974, ECLI:EU:C:1974:133.
C-33/76 *Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland,* 16.12.1976, ECLI:EU:C:1976:188.
C-45/76 *Comet BV v Produktschap voor Siergewassen,* 16.12.1976. ECLI:EU:C:1976:191.
C-106/77 *Amministrazione Delle Finanze Dello Stato and Simmenthal S.p.A.*, 9.3.1978, ECLI:EU:C:1978:49.
C-53/81 *D.M. Levin v Staatssecretaris van Justitie,* 23.3.1982, ECLI:EU:C:1982:105.
C-283/81 *Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health,* 6.10.1982, ECLI:EU:C:1982:335.
C-327/82 *Ekro BV Vee-en Vleeshandel, Apeldoorn, v. Produktschap voor Vee en Vlees, Rijswijk,* 18.1.1984, ECLI:EU:C:1984:11.
C-14/83 *Sabine von Colson and Elisabeth Kamann and Land Nordrhein-Westfalen [North-Rhine Westphalia]*, 10.4.1984, ECLI:EU:C:1984:153.
C-170/84 *Bilka-Kaufhaus GmbH v Karin Weber von Hartz,* 13.5.1986, ECLI:EU:C:1986:204.
C-222/84 *Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary, 15.5.1986,* ECLI:EU:C:1986:206.
C-66/85 *Deborah Lawrie-Blum v Land Baden-Württemberg,* 3.7.1986, ECLI:EU:C:1986:284.
C-139/85 *R. H. Kempf v Staatssecretaris van Justitie,* 3.7.1986, ECLI:EU:C:1986:158.
C-5/88 *Hubert Wachauf v Bundesamt für Ernährung und Forstwirtschaft,* 13.7.1989, ECLI:EU:C:1989:321.
C-171/88 *Ingrid Rinner-Kühn v FWW Spezial-Gebäudereinigung GmbH & Co. KG,* 13.7.1989, ECLI:EU:C:1989:328.
C-109/88 *Handels- og Kontorfunktionærernes Forbund I Danmark v Dansk Arbejdsgiverforening, acting on behalf of Danfoss,* 17.10.1989, ECLI:EU:C:1989:383.
C-215/88 *Casa Fleischhandels-GmbH v Bundesanstalt für landwirtschaftliche Marktordnung,* 13.7.1989, ECLI:EU:C:1989:331.
C-379/87 *Anita Groener v Minister for Education and City of Dublin Vocational Education Committee,* 28.11.1989, ECLI:EU:C:1989:599.
C-292/89 *The Queen v Immigration Appeal Tribunal, ex parte Gustaff Desiderius Antonissen,* 26.2.1991, ECLI:EU:C:1991:80.
C-260/89 *Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou v Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others,* 18.7.1991, ECLI:EU:C:1991:254.
C-127/92 *Dr. Pamela Mary Enderby v Frenchay Health Authority and Secretary of State for Health,* 27.10.1993 ECLI:EU:C:1993:859.
C-419/92 *Ingetraut Scholz v Opera Universitaria di Cagliari and Cinzia Porcedda,* 23.2.1994, ECLI:EU:C:1994:62.
C-180/95 *Nils Draehmpaehl and Urania Immobilienservice OHG,* 22.4.1997, ECLI:EU:C:1997:208.
C-85/96 *María Martínez Sala v Freistaat Bayern,* 12.5.1998, ECLI:EU:C:1998:217.
C-162/97 *Gunnar Nilsson, Per Olov Hageigren, Solweig Arrborn,* 19.11.1998, ECLI:EU:C:1998:554.

C-281/98 *Roman Angonese v Cassa di Risparmio di Bolzano SpA,* 6.6.2000, ECLI:EU:C:2000:296.
C-403/98 *Azienda Agricola Monte Arcosu Srl v Regione Autonoma della Sardegna, Organismo Comprensoriale No 24 della Sardegna, Ente Regionale per l'Assistenza Tecnica in Agricoltura (ERSAT),* 11.1.2001, ECLI:EU:C:2001:6.
Joined cases C-465/00, C-138/01 and C-139/01 *Rechnungshof (C-465/00) and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG, and between Christa Neukomm (C-138/01), Joseph Lauermann (C-13 9/01) and Österreichischer Rundfunk,* 20.5.2003, ECLI:EU:C:2003:294.
Joined Cases C-397/01 and 403/01, *Bernhard Pfeiffer (C-397/01), Wilhelm Roith (C-398/01), Albert Süß (C-399/01), Michael Winter (C-400/01), Klaus Nestvogel (C-401/01), Roswitha Zeller (C-402/01) and Matthias Döbele (C-403/01) v Deutsches Rotes Kreuz, Kreisverband Waldshut eV.* 5.10.2004, ECLI:EU:C:2003:245.
Joined Cases C-4/02 and C-5/02 *Hilde Schönheit v Stadt Frankfurt am Main (C-4/02) and Silvia Becker v Land Hessen (C-5/02),* 23.10.2003, ECLI:EU:C:2003:583
C-138/02 *Brian Francis Collins v Secretary of State for Work and Pensions,* 23.3.2004, ECLI:EU:C:2004:172.
C-220/03 *European Central Bank v Federal Republic of Germany,* 8.12.2005, ECLI:EU:C:2005:748.
C-278/03 *Commission of the European Communities v Italian Republic,* 12.5.2005, ECLI:EU:C:2005:281.
C-144/04 *Werner Mangold v Rüdiger Helm,* 22.10.2005, ECLI:EU:C:2005:709.
C-371/04 *Commission of the European Communities v Italian Republic,* 26.10.2006, ECLI:EU:C:2006:668.
C-13/05 *Sonia Chacón Navas v Eurest Colectividades SA,* 11.7.2006, ECLI:EU:C:2006:456.
C-438/05 *International Transport Workers' Federation and Finnish Seamen's Union v Viking Line ABP and OÜ Viking Line Eesti,* 11.12.2007, ECLI:EU:C:2007:772.
C-341/05 *Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet, Svenska Byggnadsarbetareförbundets avdelning 1, Byggettan and Svenska Elektrikerförbundet,* 18.12.2007, ECLI:EU:C:2007:809.
C-195/06 *Kommunikationsbehörde Austria (KommAustria) v Österreichischer Rundfunk (ORF),* 18.10.2007, ECLI:EU:C:2007:613.
C-268/06 *Impact v Minister for Agriculture and Food, Minister for Arts, Sport and Tourism, Minister for Communications, Marine and Natural Resources, Minister for Foreign Affairs, Minister for Justice, Equality and Law Reform, Minister for Transport,*15.4.2008, ECLI:EU:C:2008:223.
C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU,* 29.1.2008, ECLI:EU:C:2008:54.
C-303/06 *S. Coleman v Attridge Law and Steve Law,* 17.7.2008, ECLI:EU:C:2008:415.
C-524/06 *Heinz Huber v. Bundesrepublik Deutschland,* 16.12.2008, ECLI:EU:C:2008:724.
C-54/07 *Centrum voor gelijkheid van kansen en voor racismebestrijding v Firma Feryn NV,* 10.7.2008, ECLI:EU:C:2008:397.
C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,* 16.12.2008, ECLI:EU:C:2008:727.
C-229/08 *Colin Wolf v Stadt Frankfurt am Main,* 12.1.2010, ECLI:EU:C:2010:3.
C-314/08 *Krzysztof Filipiak v Dyrektor Izby Skarbowej w Poznaniu,* 19.11.2009, ECLI:EU:C:2009:719.
C-499/08 *Ingeniørforeningen i Danmark v Region Syddanmark,* 12.10.2010, ECLI:EU:C:2010:600.
C-92/09 and C-93/09 joined cases *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen,* 9.10.2010, ECLI:EU:C:2010:662.
C-236/09 *Association belge des Consommateurs Test-Achats ASBl, Yann van Vugt, Charles Basselier v Conseil des ministers,* 1.3.2011, ECLI:EU:C:2011:100.

C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), intervening parties: Belgian Entertainment Association Video ASBL (BEA Video), Belgian Entertainment Association Music ASBL (BEA Music), Internet Service Provider Association ASBL (ISPA),* 24.11.2011, ECLI:EU:C:2011:771.

C-104/10 *Patrick Kelly v National University of Ireland (University College, Dublin),* 21.7.2011, ECLI:EU:C:2011:506.

C-415/10 *Galina Meister v Speech Design Carrier Systems GmbH,* 19.4.2012, ECLI:EU:C:2012:217.

C-617/10 *Åklagaren v Hans Åkerberg Fransson,* 26.2.2013, ECLI:EU:C:2013:105.

Joined Cases C-335/11 and C-337/11 *HK Danmark, acting on behalf of Jette Ring v Dansk almennyttigt Boligselskab (C-335/11) and HK Danmark, acting on behalf of Lone Skouboe Werge v Dansk Arbejdsgiverforening, acting on behalf of Pro Display A/S (C-337/11),* 11.4.2013, ECLI:EU:C:2013:222.

C-399/11 *Stefano Melloni v Ministerio Fiscal,* 26.2.2013, ECLI:EU:C:2013:107.

C-426/11 *Mark Alemo-Herron and Others v Parkwood Leisure Ltd,* 18.7.2013, ECLI:EU:C:2013:521.

C-476/11 *HK Danmark v Experian A/S, intervener: Beskæftigelsesministeriet*, 26.9.2013, ECLI:EU:C:2013:590.

C-81/12 *Asociaţia Accept v Consiliul Naţional pentru Combaterea Discriminării,* 25.4.2013, ECLI:EU:C:2013:275.

C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* 13.5.2014, ECLI:EU:C:2014:317.

C-176/12 *Association de médiation sociale v Union locale des syndicats CGT and Others,* 15.1.2014, ECLI:EU:C:2014:2.

C-267/12 *Frédéric Hay v Crédit agricole mutuel de Charente-Maritime et des Deux-Sèvres,* 12.12.2013, ECLI:EU:C:2013:823.

Joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General, intervener: Irish Human Rights Commission, and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others,* 8.4.2014, ECLI:EU:C:2014:238.

C-356/12 *Wolfgang Glatzel v Freistaat Bayern,* 22.5.2014, ECLI:EU:C:2014:350.

C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others,* 7.10.2013, ECLI:EU:C:2013:715.

C-206/13 *Cruciano Siragusa v Regione Sicilia — Soprintendenza Beni Culturali e Ambientali di Palermo,* 6.3.2014, ECLI:EU:C:2014:126.

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others,* 8.4.2014, ECLI:EU:C:2014:238.

C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů,* 11.12.2014 ECLI:EU:C:2014:2428.

C-354/13 *Fag og Arbejde (FOA), Acting on Behalf of Karsten Kaltoft, v. Kommunernes Landsforening (KL), Acting on Behalf of the Municipality of Billund,* 18.12.2014, ECLI:EU:C:2014:2463.

C-416/13 *Mario Vital Pérez v Ayuntamiento de Oviedo,* 13.11.2014, ECLI:EU:C:2014:2371.

C-83/14 *CHEZ Razpredelenie Bulgaria AD v. Komisia za zashtita ot diskriminatsia, third parties: Anelia Nikolova, Darzhavna Komisia za energiyno i vodno regulirane,* 16.7.2015, ECLI:EU:C:2015:480.

C-258/14 *Eugenia Florescu, Ioan Poiană, Cosmina Diaconu, Anca Vidrighin, Eugenia Elena Bădilă v Casa Județeană de Pensii Sibiu, Casa Națională de Pensii și alte Drepturi de Asigurări Sociale, Ministerul Muncii, Familiei și Protecției Sociale, Statul roman, Ministerul Finanțelor Publice,* 13.7.2017, ECLI:EU:C:2017:448.

C-317/14 *European Commission v Kingdom of Belgium,* 5.2.2015, ECLI:EU:C:2015:63.

C-362/14 *Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd,* 6.10.2025, ECLI:EU:C:2015:650.

C-441/14 *Dansk Industri (DI), acting on behalf of Ajos A/S, v Estate of Karsten Eigil Rasmussen,* 19.4.2016, ECLI:EU:C:2016:278.
C-157/15 *Samira Achbita and Centrum voor gelijkheid van kansen en voor racismebestrijding v G4S Secure Solutions NV,* 14.3.2017, ECLI:EU:C:2017:203.
C-188/15 *Asma Bougnaoui, Association de défense des droits de l'homme (ADDH) v Micropole SA, formerly Micropole Univers SA,* 14.3.2017, ECLI:EU:C:2017:204.
C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen, and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis, 21.12.2016,* ECLI:EU:C:2016:970.
C-258/15 *Gorka Salaberria Sorondo v Academia Vasca de Policía y Emergencias,* 15.11.2016, ECLI:EU:C:2016:873.
C-406/15 *Petya Milkova v Izpalnitelen direktor na Agentsiata za privatizatsia i sledprivatizatsionen control,* 9.3.2017, ECLI:EU:C:2017:198.
C-423/15 *Nils-Johannes Kratzer v R+V Allgemeine Versicherung AG*, 28.7.2016, ECLI:EU:C:2016:604.
C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme",* 4.5.2017, ECLI:EU:C:2017:336.
C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, interveners: Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht,* 5.6.2018, ECLI:EU:C:2018:388.
C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.,* 17.4.2018, ECLI:EU:C:2018:257.
C-434/16 *Peter Nowak v Data Protection Commissioner,* 20.12.2017, ECLI:EU:C:2017:994.
Joined cases C-569/16 and C-570/16 *Stadt Wuppertal v Maria Elisabeth Bauer (C-569/16) and Volker Willmeroth, in his capacity as owner of TWI Technische Wartung und Instandsetzung Volker Willmeroth e.K. v Martina Broßonn (C-570/16),* 6.11.2018, ECLI:EU:C:2018:871.
C-684/16 *Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV v Tetsuji Shimizu,* 6.11.2018, ECLI:EU:C:2018:874.
C-25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta,* 10.7.2018, ECLI:EU:C:2018:551.
C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, interveners: Facebook Ireland Ltd, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen,* 29.7.2019, ECLI:EU:C:2019:629.
C-136/17 *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL), interveners: Premier ministre, Google LLC, successor to Google Inc.,* 24.9.2019, ECLI:EU:C:2019:773.
C-193/17 *Cresco Investigation GmbH v Markus Achatzi,* 22.1.2019, ECLI:EU:C:2019:43.
C-496/17 *Deutsche Post AG v Hauptzollamt Köln,* 16.1.2019, ECLI:EU:C:2019:26.
C-507/18 *NH v Associazione Avvocatura per i diritti LGBTI - Rete Lenford,* 23.4.2020, ECLI:EU:C:2020:289.
C-610/18 *AFMB Ltd and Others v Raad van bestuur van de Sociale verzekeringsbank,* 16.7.2020, ECLI:EU:C:2020:565.
C-16/19 *VL v Szpital Kliniczny im. dra J. Babińskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Krakowie,* 26.1.2021, ECLI:EU:C:2021:64.
C-370/19 *Irish Ferries Ltd v National Transport Authority,* 2.9.2021, ECLI:EU:C:664.
C-741/19 *Republic of Moldova v Komstroy LLC, successor in law to the company Energoalians,* 2.9.2021, ECLI:EU:C:2021:655.
C-184/20 *OT v Vyriausioji tarnybinės etikos komisija, third party: Fondas 'Nevyriausybinių organizacijų informacijos ir paramos centras',* 1.8.2022, ECLI:EU:C:2022:601.
C-154/21 *RW v Österreichische Post AG,* 12.1.2023, ECLI:EU:C:2023:3.
C-300/21 *UI v Österreichische Post AG,* 4.5.2023, ECLI:EU:C:2023:370.

C-487/21 *F.F. v Österreichische Datenschutzbehörde, intervener: CRIF GmbH,* 4.5.2023, ECLI:EU:C:2023:369.
C-579/21 *J.M., intervener: Apulaistietosuojavaltuutettu, Pankki S,* 22.6.2023, ECLI:EU:C:2023:501.
C-252/21 *Meta Platforms Inc and Others v Bundeskartellamt,* 4.7.2023, ECLI:EU:C:2023:537.
C-430/21 *RS,* 22.2.2022, ECLI:EU:C:2022:99.
C-446/21 *Maximilian Schrems v Meta Platforms Ireland Limited,* 4.10.2024, ECLI:EU:C:2024:834.
C-588/21 *Public.Resource.Org and Right to Know v Commission and Others*, 5.3.2024, ECLI:EU:C:2024:201.
C-634/21 *OQ v Land Hessen, intervener: SCHUFA Holding AG*, 7.12.2023, ECLI:EU:C:2023:957.
C-667/21 *ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts,* 21.12.2023, ECLI:EU:C:2023:1022.
C-687/21 *BL v MediaMarktSaturn Hagen-Iserlohn GmbH,* 25.1.2024, ECLI:EU:C:2024:72.
C-203/22 *CK v Magistrat der Stadt Wien, other party: Dun & Bradstreet Austria GmbH,* 27.2.2025, ECLI:EU:C:2025:117.
C-456/22 *VX, AT v Gemeinde Ummendorf,* 14.12.2023, ECLI:EU:C:2023:988.
C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit,* 7.3.2024, ECLI:EU:C:2024:214.
C-21/23 *ND v DR (Lindenapotheke),* 4.10.2024, ECLI:EU:C:2024:846.
C-196/23 *CL and Others v DB and Fondo de Garantía Salarial (FOGASA) - Plamaro,* 11.7.2024, ECLI:EU:C:2024:596.
C-394/23 *Mousse v Commission nationale de l'informatique et des libertés (CNIL), SNCF Connect,* 9.1.2025, ECLI:EU:C:2025:2.
C-507/23 *A v Patērētāju tiesību aizsardzības centrs,* 4.10.2024, ECLI:EU:C:2024:854.
C-655/23 *IP v Quirin Privatbank AG,* 4.9.2025, ECLI:EU:C:2025:655.

Supreme Court of Finland

KKO:2015:41
KKO:2025:50

Supreme Administrative Court of Finland

KHO:2025:51

Appendices

Appendix I – Framework of key legal parameters for algorithmic recruitment system use

FRAMEWORK OF KEY LEGAL PARAMETERS FOR ALGORITHMIC RECRUITMENT SYSTEM USE

	TYPE OF LEGAL PARAMETER			
TYPE OF RECRUITMENT SYSTEM	**BAN**	**OBLIGATION**	**SPECIFIC DUTY**	**ACTIONABLE RIGHT**
ALL ALGORITHMIC RECRUITMENT SYSTEMS	Prohibition of asking pay history. (PTD Art. 5(2))***	Ensuring a lawful basis for processing job applicants' personal data in the ARS exists (CFREU Art. 8, GDPR Art. 6)	Data protection impact assessment (GDPR Art. 35) and prior consultation if high-risk remains (GDPR Art. 36).	Right of access (GDPR Art. 15, CFREU Art. 8(2))
	Prohibition of direct and indirect discrimination (CFREU Art. 21, RED and EED Art. 2, GED Art. 14)	Demonstrating that the ARS complies with the principles relating to processing of personal data, that is, with the requirements of (a) lawfulness, fairness and transparency, (b) purpose limitation, (c) data minimisation, (d) accuracy, (e) storage limitation, and (f) integrity and confidentiality. (GDPR Art. 5)		Right to rectification (GDPR Art. 16, CFREU Art. 8(2))
	Prohibition of processing special category personal data (GDPR Art. 9)	Compliance with the data subject rights and transparency (GDPR Arts. 12-14).		Rights to erasure, restriction of processing and data portability (GDPR Arts. 17-20)
	Prohibition of processing personal data relating to criminal convictions and offences (GDPR Art. 10)	Accessibility features and potential for reasonable accommodations (EED Art. 5)		Right to object (GDPR Art. 21)

FRAMEWORK OF KEY LEGAL PARAMETERS FOR ALGORITHMIC RECRUITMENT SYSTEM USE

	TYPE OF LEGAL PARAMETER			
TYPE OF RECRUITMENT SYSTEM	**BAN**	**OBLIGATION**	**SPECIFIC DUTY**	**ACTIONABLE RIGHT**
AI SYSTEMS (AIA Art. 3, point 1)	Prohibition of certain AI practices - e.g. decision manipulation, exploitation of vulnerabilities, social scoring, or biometric categorisation (AIA Art. 5(1)(a), (b), (c), and (g))	Transparency of the ARS's direct interactions with job applicants and marking of artificially generated content. (AIA Art. 50* / GDPR Art. 5(1)(a))	Ensuring a sufficient level of AI literacy of staff and other persons operating AI systems (AIA Art. 4)	
	Prohibitions of criminal risk assessment and emotion inference in the workplace (AIA Art. 5(1)(d) and (f))			
High-risk AI systems (AIA Art. 6(2) and Annex III, point 4(a))		CE-marking. (AIA Art. 48* / GDPR Art 5(1)(a))	Technical and organisational measures to ensure compliance with the provider's instructions for use of the ARS (AIA Art. 26(1) and Art. 13(1))**	
		Registration in the EU database for high-risk AI systems (AIA Art. 49 and 71* / GDPR Art. 5(1)(a))	Assigning a competent person to oversee the ARS and providing support for them. (AIA Art. 26(2) and Art. 14)**	
			Input data under the employer's control to be relevant and sufficiently representative (AIA Art. 26(4))**	

FRAMEWORK OF KEY LEGAL PARAMETERS FOR ALGORITHMIC RECRUITMENT SYSTEM USE

	TYPE OF LEGAL PARAMETER			
TYPE OF RECRUITMENT SYSTEM	**BAN**	**OBLIGATION**	**SPECIFIC DUTY**	**ACTIONABLE RIGHT**
			Monitoring the ARS's operation (AIA Art. 26(5))**	
			Informing providers, importers, distributors and market surveillance authorities about risks and serious incidents and suspending the use of the system (AIA Art. 26(5) and Art. 73)**	
			Log keeping (AIA Art. 26(6))**	
			Informing workers' representatives and the affected workers that they are subject to the use of ARS. (AIA Art. 26(7))**	
			[Fundamental rights impact assessments, only for certain employers providing public services, (AIA Art. 27).]**	
High-risk AI systems that assist in individual decision-making (AIA Arts. 26(11) and 86)			Informing job applicants that they are subject to the use of the ARS (AIA Art. 26(11))**	Right to explanation of decisions producing legal effects or similarly significantly adversely affecting job applicants (AIA Art. 86)*

FRAMEWORK OF KEY LEGAL PARAMETERS FOR ALGORITHMIC RECRUITMENT SYSTEM USE

	TYPE OF LEGAL PARAMETER			
TYPE OF RECRUITMENT SYSTEM	**BAN**	**OBLIGATION**	**SPECIFIC DUTY**	**ACTIONABLE RIGHT**
SYSTEMS USING ADM (GDPR Art. 22)	Prohibition of individual automated decision-making (GDPR Art. 22)	Suitable safeguard measures (GDPR Art. 22(3), Recital 71)	Informing of the existence of ADM, its logic, significance and envisaged consequences (GDPR Art. 13(2)(f), 14(2)(g) and 15(1)(h).	Right to explanation (GDPR Art. 15(1)(h), Recital 71)
				Right to obtain human intervention, express their point of view and contest the decision (GDPR Art. 22(3))
* Applicable as of 2nd August 2026 (to prior systems only if substantially modified) ** Applicable as of 2nd August 2026, unless Digital Omnibus on AI postpones the applicability up until 2 December 2027 (to prior systems only if substantially modified) *** To be implemented in Member State legislation by 7 June 2026	Absolute prohibitions of certain practices Prohibitions of certain practices, with specified exceptions	Compliance requirements affecting ARSs that users must ensure are complied with	Requirements imposed on employers that require proactive measures and are triggered due to the use of an ARS	Job applicants' rights that require their proactivity to be triggered

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

Painosalama, Turku, Finland 2026

ISBN 978-952-02-0679-6 (PRINT)
ISBN 978-952-02-0680-2 (PDF)
ISSN 0082-6987 (Print)
ISSN 2343-3191 (Online)