UNIVERSITY OF TURKU
Turku School of Economics

Supporting Small and Medium Enterprises in AI Development: The Role of EU AI Regulatory Sandboxes

Information Systems Science

Master's thesis

Author:
Eeva Kaakkurivaara

Supervisor:
KTT Jukka Heikkilä

4.7.2025

Turku

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

Master's thesis

Subject: Information Systems Science
Author: Eeva Kaakkurivaara
Title: Supporting Small and Medium Enterprises in AI Development: The Role of EU AI Regulatory Sandboxes
Supervisor: KTT Jukka Heikkilä
Number of pages: 95 pages + appendices 3 pages
Date: 4.7.2025

Small and medium-sized enterprises (SMEs) make up a large portion of the global economy and their contribution to innovation, employment and economic growth is significant. Artificial intelligence (AI) is rapidly spreading, and it has created opportunities for productivity and innovation. The limited resources of SMEs often hinder their ability to develop and adopt new AI innovations which could be a significant competitive disadvantage. The newly developed AI legislation by the European Union, the AI Act, introduces a framework for AI regulatory sandboxes which are designed to help companies, especially SMEs and start-ups, to safely develop and test new AI technologies without regulatory barriers. Regulatory sandboxes have been used the fields of financial technology and privacy, and they have been shown to have several beneficial aspects for companies. The purpose of this thesis is to research whether the AI regulatory sandboxes presented in the EU AI Act could aid SMEs in AI development and innovation.

In this thesis the challenges of European competitiveness are presented followed by digital transformation in SMEs. After that, the basis for the EU AI Act and the Act itself are presented followed by current AI regulations. Next the thesis goes more deeply into the existing regulatory sandboxes followed by the empirical part of this thesis. It consists of analysing two questionnaires which aim to map out the attitudes of SMEs towards AI development, AI regulation and the AI regulatory sandboxes.

European competitiveness faces challenges, and Europe is falling behind in the tech market while the United States and China are making advancements. SMEs, taking up a large share of the European economy, are important to consider when trying to improve the competitiveness of Europe. Innovation adoption, which would accelerate growth, is often difficult for SMEs as they do not possess the needed resources. Due to the risks that artificial intelligence poses, EU has taken an initiative to develop a comprehensive AI regulation, the AI Act. The AI Act applies to the EU market and actors operating in the market using AI must comply with it. The AI Act includes a framework for the regulatory sandbox and taking into consideration the limited resources of SMEs EU has provided them with a free access to the sandbox.

Regulatory sandboxes from the fields of financial technology and privacy have been shown to have benefits for companies such as facilitated market entry and they have helped especially smaller companies to navigate the complex regulatory environment. However, they have possible risks for example for competition and consumers if not designed and managed properly. Results from the empirical part of this thesis show that the regulatory sandbox for artificial intelligence can offer help to SMEs in navigating the regulatory environment and thus develop more trustworthy AI solutions as well as provide regulatory guidance for SMEs. The sandbox can offer a safe environment to develop test and validate AI innovations as well as allows for better communication and cooperation between different actors such as companies and regulators.

Key words: artificial intelligence, AI, AI regulation, AI regulatory sandbox, EU AI Act, fintech, innovation, regulatory sandbox, SME.

TABLE OF CONTENTS

LIST OF FIGURES

List of terms

artificial intelligence (AI). A system designed by humans to collect and interpret data to solve a complex problem. An algorithm based decision-making system, or a group of computer programs designed for problem solving. (European Commission, 2019b; Bathaee, 2018.)

AI system. A machine-based system that can operate independently on some level, can adapt and make decisions, predictions, content or recommendations from the input it receives (EU, 2024).

deployer. A natural or legal person or a public actor that uses an AI system that it is responsible for except if it is in personal use (EU, 2024).

developer. An entity that codes, designs or produces artificial intelligence systems (Business Software Alliance, 2023).

financial technology (fintech). Use of technology to provide innovative financial services ("financial technology (fintech)", 2025).

general-purpose AI model. An AI model that exhibits generality, can perform wide range of different tasks and can be integrated into many different downstream systems (EU, 2024).

innovation. A new method or an idea or creation and use of a new method or an idea ("innovation", 2025).

multistakeholderism. The participation and collaboration of different actors such as policymakers, researchers, industry representatives and the public that provide different perspectives and experiences (EC-OECD, 2025).

provider. A natural or legal person or public actor that develops or has developed AI system or a general-purpose AI model and puts it on the market or into service under its own name (EU, 2024).

regulation. An official law or rule ("regulation", 2025).

regulatory sandbox. A controlled, real-world environment that allows testing of innovations under the supervision of a competent authority (European Commission, 2023).

small and medium-sized enterprise (SME). An enterprise that has less than 50 million euros in turnover or less than 43 million euros in revenue and less than 250 employees (European Commission: SME definition).

systemic risk. Risk posed by the general-purpose AI models that can have a notable impact on the Union market and that can negatively affect the public (EU, 2024).

1 Introduction

1.1 Background

European competitiveness faces many challenges, and the European market is in danger of falling behind its biggest competitors, the United States and China. The share of European Union (EU) in global trade is decreasing and disruptive technologies are facing decline. Europe has no policy actions to support common objectives and lacks collaboration regarding innovation and its investment. EU has also faced criticism for its regulatory environment that hinders innovation, especially small and medium-sized enterprises (SMEs) and start-ups face major challenges with regulatory barriers. (Draghi, 2024.)

According to the European Commission (EC), small and medium-sized enterprises are defined as having less than 50 million euros in turnover or less than 43 million euros in revenue and having less than 250 employees (European Commission: SME definition). The global economy largely consists of SMEs, around 90% of the world's businesses are SMEs and they employ more than 50% of all employees worldwide (Iyelolu et al., 2024). Their contribution to innovation, employment and economic growth is notable (Muminova et al., 2024).

The quickly spreading artificial intelligence (AI) has created opportunities for innovation and increased productivity that could help Europe in enhancing its competitiveness on the global market. However, the regulatory barriers that affect especially SMEs regarding innovation need to be addressed. (Draghi, 2024.) Inconsistent and complex policies can hinder innovation adoption in SMEs, especially if their legal and administrative resources are limited. Governments and other policymakers have the potential to help SMEs adopt AI innovations by creating supporting regulatory environments and providing financial incentives. (Iyelolu et al., 2024.) The EU intends to improve the business practices of SMEs and ensure that they are aligned with current technologies as the economic stability is influenced by the competitiveness of SMEs (Schwaeke et al., 2024).

The EU introduced the AI Act in 2021 for AI regulation which includes a "sandbox" framework for fostering AI innovation across the EU (Madiega & De Pol, 2022). These sandboxes can be defined as "schemes that enable firms to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority" (European Commission, 2023). According to the Council of the European Union, regulatory sandboxes can provide notable opportunities for innovation and growth, especially in SMEs. Experimenting within the boundaries

of the sandbox can help companies adapt to the framework and simultaneously discover possible flaws in the regulation itself. (Pošćić & Martinović, 2022.)

1.2 Research questions

It is still unclear how the AI sandboxes can encourage innovation in SMEs. The question is whether the benefits and opportunities will be greater than the cost of regulatory compliance (Pošćić & Martinović, 2022). The aim of this study is to find out whether the AI regulatory sandboxes have a clear benefit in AI development in SMEs. The main research question of this study is:

RQ: What possible effects could the AI regulatory sandbox have on AI development in SMEs?

In order to better answer this question, this study also includes two auxiliary research questions:

ARQ1: What possible challenges could SMEs face in accessing and utilizing sandbox models effectively?

ARQ2: What specific tools and support can sandboxes offer to SMEs?

1.3 Motivation

AI has the potential to help companies develop processes, produce new products and services and better understand customers (Jafarzadeh et al., 2024). Implementation of AI solutions in SMEs has the potential to significantly improve their operations, reduce costs and enhance strategic planning. Additionally, they can facilitate the automation of repetitive tasks and consequently free up human resources for more complex business practices. (Iyelolu et al., 2024.) This can subsequently lead to better employee experience (Schwaeke et al., 2024).

It has also been recognized that adopting AI technologies brings new market opportunities for companies (Chatterjee et al., 2022). Innovation in SMEs allows them to improve their product and service offerings which helps them meet evolving customer needs and improve their position in the competitive market. Innovation is crucial for SMEs to adapt to changing markets and external shocks. (Iyelolu et al., 2024.)

However, AI adoption in SMEs has its challenges such as limited resources and skills to fully understand the potential of AI (Jafarzadeh et al., 2024; Wei & Pardo, 2022). Other issues include uncertainty about the benefits of AI, the necessary initial investment, changes in the operations of the company and uncertainty about how it’s going to affect the jobs of the employees (Jafarzadeh et

al., 2024). Insufficient technical knowledge and lack of access to external networks are also barriers for AI adoption in SMEs. AI systems require knowledge in, for example, machine learning, software engineering and data science. SMEs often don't have experts in these areas and face challenges in attracting skilled individuals. Concerns about data security and privacy are also notable challenges for SMEs when adopting AI innovations. Access to large amounts of data is usually essential for the effective use of AI, however, this raises concerns about compliance with regulations and data protection. (Iyelolu et al., 2024.)

The idea of regulatory sandboxes included in the EU AI Act is to allow the testing and building of new inventions in a regulatory environment within the controlling boundaries but without restrictive regulations that hinder innovation. They act as a space for experimentation of innovative technologies. (Pošćić & Martinović, 2022.) Regulatory sandboxes have existed before the EU AI Act and they have especially been popular in the financial technology (fintech) industry. In 2016, the UK's Financial Conduct Authority (FCA) introduced the regulatory sandbox for the financial technology sector. After that, many regulators around the world have adopted the sandbox model in their own business practices. (Sky, 2024.) These countries include Hong Kong, Singapore, Australia, India, Malaysia, Japan and Canada. It has been researched that the adoption of the sandbox model can foster innovation, at least in the fintech industry, by promoting investment and reducing legal risks by eliminating uncertainty. (Goo & Heo, 2020.)

1.4 Research method and theoretical framework

This thesis is done as a combination of literature review and survey research. A literature review was done first as it provides the context for the research questions and theoretical background for the empirical part. A literature review is usually done to better understand the existing research done on the subject and to establish the research problem. (Paré et al., 2015.) Articles and materials for the literature review was collected using Google Scholar and Scopus database using search terms such as "artificial intelligence", "AI", "AI regulation", "AI regulatory sandbox", "EU AI Act", "innovation", "regulatory sandbox", "SME" and "SME and AI regulation". Reliability and validity of the articles and materials was evaluated by reviewing the author or authors, platform of the publication, references and citations of the publication, time of publication, accuracy, possible peer-review and the reliability and validity of the journals was in some cases checked through the Cabells database. A comprehensive description of the survey research is presented in the methodology chapter.

This study utilises the technology–organization–environment (TOE) framework first created by Tornatzky (Tornatzky & Fleischer, 1990). This framework illustrates the internal and external factors that influence decisions regarding technology adoption in organizations (Schwaeke et al., 2024). The framework provides a basis for a systematic examination of the various factors influencing AI adoption in SMEs by identifying three perspectives: technological, organizational and environmental. The technological viewpoint focuses on the role and relevance of technologies, the organizational perspective refers to issues related to the structure of the organization and the managerial perspective, and lastly the environmental viewpoint refers to the external factors such as the competitive market and government policies and regulations. (El-Haddadeh, 2020.) Prior research has shown that the TOE framework is appropriate for studying and analyzing the dynamics affecting technological adoption in organizations (Schwaeke et al., 2024).

In this study the focus is mainly on the external factors, more specifically on the regulations issued by the EU as the goal of this study is to examine how the regulatory sandboxes affect the AI innovation adoption in SMEs. This study also focuses more on experimental regulation than traditional regulation as the regulatory sandbox is a form of experimental regulation (Ruschemeier, 2025).

2 European competitiveness and technological adoption in SMEs

2.1 Challenges of European competitiveness

The European Union has faced a lot of criticism regarding its regulatory landscape. Critics and scholars claim that EU's regulatory approach has hindered innovation and that regulation is the reason for Europe lagging behind the US and China when it comes to successful tech companies. Regulation is said to increase companies' compliance costs, and this can direct companies' resources away from for example research and development (R&D) activities and thus hinder innovation. Especially SMEs and start-ups face great challenges regarding complex regulatory policies. However, other reasons for Europe's bad success compared to the US and China, especially in the tech industry have been discussed. (Bradford, 2024; Draghi, 2024.)

One of the main challenges Europe has regarding competitiveness is that there are common objectives, however, no policy actions or priorities to support those objectives. The fragmentation of the Single Market also has costly effects on the European competitiveness, it pushes high-growth companies out of Europe which consequently hinders the growth of Europe's capital markets and prevents Europeans from growing their wealth. This fragmentation has also been claimed to restrict the scaling of new innovations in the European Union. Additionally, Europe lacks collaboration when it comes to innovation despite breakthrough technologies demanding large investment. For example, the US and the public sector in the EU spend the same amount as a share of GDP on research and innovation (R&I) but only 10% of this happens at the EU level. (Bradford, 2024; Draghi, 2024.)

Europe desperately needs to accelerate innovation and improve its competitiveness on the global market. The foreign demand of EU companies is declining, and they are facing increasing competition from especially Chinese companies and the share that the EU companies hold in global trade is decreasing. Moreover, decline is occurring in future shaping advanced technologies as well, from 2013 to 2023 EU's share of worldwide tech revenues went from 22% to 18% and the US share went from 30% to 38%. In addition, out of the 50 biggest tech companies in the world only four are European. (Draghi, 2024.)

Accelerating innovation is an urgent issue for Europe to raise productivity growth in the EU which in turn would increase household income and domestic demand. Europe must work fast and seize the opportunities created by the rapid spread of artificial intelligence in increasing innovation and productivity. In order to accelerate the rate of innovation, Europe needs to close the innovation gap

which will allow growth in scientific and technological innovation, remove barriers from innovative companies and allow more innovations to reach commercialisation. Europe is greatly behind the US in breakthrough digital innovations which can be seen from their share of 70% of foundational AI models developed since 2017. (Draghi, 2024.)

Another issue is the static industrial structure of Europe compared to the US that is constantly investing in new emerging technologies. For instance, Europe's top three R&I spenders have been automotive companies for decades versus the US' major R&I spenders changing throughout the decades from automotive to software and hardware to the digital sector all of which have had high growth potential. The R&I spending in Europe would need to be sufficiently directed at breakthrough and disruptive innovation. (Draghi, 2024.) According to Anu Bradford, EU's insufficiently developed capital markets also contribute to tech companies' inability to thrive in the EU as do the EU's laws on bankruptcy that focus on penalty instead of giving a second chance. Bradford also argues that EU's current policies on immigration prevent foreign tech talent from coming into Europe and starting companies there. (Bradford, 2024.)

Europe also needs to address the regulatory barriers prohibiting innovation which especially affect SMEs. The fragmented nature of the EU regulatory landscape and expensive and complex procedures hinder innovators' ability to file Intellectual Property Rights which complicates young companies' entry to the Single Market. Additionally, the abundance of tech-focused legislation makes it difficult for especially SMEs to navigate the regulatory landscape. Establishing large, integrated data sets that can be used to train AI models is also costly due to the EU's limitation on data processing and storing. High compliance costs result in smaller companies not being able to operate in the EU area. (Draghi, 2024.)

2.2 What drives digital transformation in SMEs

In today's economy, digital technologies are becoming more and more integrated into different processes and functions across industries. Simultaneously digital technology innovations are an important factor for economic growth and a competitiveness. (Sima et al., 2020.) Due to the rapid adoption of digital technologies by more and more companies, the market situation changes constantly, and companies must find ways to adapt to these changes (Brodny & Tutak, 2022).

SMEs play an important role in the economy and in the EU, they account for as much as 99% of all companies. SMEs also generate over 50% of the European GDP and employ around 100 million people. Due to their role in the economy, it is very important for SMEs to adapt to the rapidly

changing environment of digital and technological development. However, due to their limited resources both financial and human, this could be quite challenging. Large investment, sufficient human resources and adequate time are needed in the development of digital innovation. (Brodny & Tutak, 2022; Ingaldi & Ulewicz, 2020.)

Several studies have shown that SMEs often have limited resources, such as financial and human resources, which contributes to numerous challenges for them during the technological transformation process (Brodny & Tutak, 2022; Horváth & Szabó, 2019; Müller et al., 2018). SMEs also often lack technological and organisational resources such as knowledge management and digital networking. SMEs specifically need these resources to fundamentally transform their operations which is often required in order to successfully adapt to the new technological environment. (Omrani et al., 2022.)

Crockett et al. (2021) in their study found that main barriers for SMEs to adopt toolkits that would aid in ethical AI development were lack of available resources such as staff, time and skill, doubt about involving public stakeholders in the design process of new products, insufficient understanding of responsibility and accountability governance around AI, lack of compliance and audit, insufficient knowledge about legal frameworks, ethics and data, communication challenges with users due to for example a language barrier and what are the consequences regarding liability for example the consequences of non-compliance aren't clear. (Crockett et al., 2021.)

Omrani et al. (2022) conducted a study which included over 15 000 SMEs worldwide to analyse the factors that influence technological adoption in SMEs. They found that organizational and technological factors play a major role in technology adoption. Especially, company's innovation level, availability of technological tools and the support for technology adoption through corporate regulation were shown to have major importance. (Omrani et al., 2022.)

The current technological situation of a company includes the internal practices and equipment and the external technological tools that are available to the company. Proper IT infrastructure, previous exposure to and the perceived benefit of digital technology greatly influence the adoption of digital technologies in SMEs. (El-Haddadeh et al., 2021; Mahroof, 2019; Omrani et al., 2022.) Factors that indicate AI readiness are resources, strategic alignment, culture, knowledge and data (Jöhnk et al., 2021). Additionally, customer demands can be a catalyst for technological adoption as well as the company wanting to set an innovative image. Studies have shown that technological knowledge and resources as well as perceived benefits are main factors for companies to adopt big data. However,

environmental and organizational factors indirectly affect big data adoption by enhancing support from top management. (El-Haddadeh et al., 2021; Omrani et al., 2022.)

Regulations issued at a national level and government support also have the potential to influence the development of new digital technologies such as AI (Chen et al., 2020; Omrani et al., 2022). However, national regulatory environment alone does not provide sufficient basis for technology adoption and digital transformation. They also call for digital resources, technological knowledge as well as organizational support. Additionally, encouraging policies play a vital role in the adoption process and decision. The environmental context seems to have a smaller impact on the decision to adopt new technologies than the technological and organisational contexts. Moreover, the internal factors such as existing IT infrastructure impact the adoption decision significantly more than external factors such as government regulation, competition and industry characteristics. (Omrani et al., 2022).

3 Basis for the EU AI Act

3.1 Why is AI regulation needed

Artificial intelligence (AI) is defined by the EU's High-Level Expert Group as systems designed by humans that collect and interpret data to solve a complex problem such as robotics, machine reasoning and machine learning (European Commission, 2019b). AI can also be defined as a group of computer programs that are designed for problem solving that requires deductive reasoning, using uncertain or incomplete data to make decisions, optimization, perception and classification (Bathaee, 2018). The term AI is usually used when talking about algorithm-based decision-making systems. These systems cause special challenges to legal regulation for many reasons. Typical features of AI systems include irreversibility and thus AI systems could have irreversible negative consequences for humanity. (Caruana & Borg, 2024; Ruschemeier, 2025.) At the moment AI has the ability to obtain, process and interpret vast amounts of data, use this data to make decisions and act based on these decisions (Ufert, 2020).

Large amounts of digital technologies have an information deficit which, for example, means that the trail from input to output isn't 100% traceable in some decision-making algorithms. This could be caused by the complexity of the calculation or the volume of data. (Ruschemeier, 2025.) AI's ability to self-learn combined with its ability to learn fast and find decision paths that humans haven't even come across makes it capable of finding connections and correlations within data sets without addressing the causation. Therefore, AI might construct solutions that are impossible to understand by humans as the reasons for the decision-making are unknown. This is also referred to as the black-box phenomenon which greatly reduces AI's explainability. (Ufert, 2020.) This information deficit results in the uncertainty of the potential risks or damages that these technologies can cause. This in turn complicates the development of regulatory frameworks. (Ruschemeier, 2025.) Frank Pasquale's book The Black Box society (2015) is one of the widely known works that discusses the black box issue from the viewpoint of regulation (Black & Murray, 2019). In his book Pasquale defines the black box as a system that inputs and outputs can be observed but the process cannot (Pasquale, 2015).

AI systems have the possibility to create numerous challenges through their impact on democracy and fundamental human rights. When integrated into products or services they could pose significant safety hazards if not regulated properly. (Caruana & Borg, 2024.) The main concerns surrounding AI from a fundamental rights perspective can be identified as discriminatory and

biased AI and they pose risks related to data protection and privacy. AI has the ability to acquire and process vast amounts of data which raises privacy concerns. AI can for example identify links among different data sets when analysing large quantities of them and this can lead to de-anonymization of said data. AI can also create discriminatory content if the training data is biased. (Ufert, 2020.)

Deceptive and/or manipulative systems could further impact societies and individuals. The possible manipulation of online platforms, which is conducted for example by automated exploitation or inauthentic use of the service or rapidly spreading and amplifying illegal content and information, combined with behaviourally targeted advertising could potentially affect and influence elections threatening the concept of democracy. Additionally, algorithmic bias can create echo chambers in the online environment and consequently prevent alternative viewpoints from accessing individual's online "bubble". (Caruana & Borg, 2024.)

AI systems are able to mass manipulate consumer weaknesses and influence the political opinions of the public. They are capable of indirect and direct discrimination and manipulation. (Ranchordás, 2021.) Unregulated AI systems also pose a threat to the structure of western societies by affecting fundamental values that these societies a based on. This could lead to breaches of fundamental rights such as right to privacy, personal data protection, self-determination, freedom of expression and non-discrimination. Judicial systems could also be affected and people's right to a fair trial could be compromised. (Caruana & Borg, 2024.)

It is evident that AI systems can have negative effects on society by causing harm and intensifying existing oppressive and discriminatory systems such as limited access to healthcare, resources or opportunities, unjust accusations of committing a crime and excess surveillance (Sloane & Wüllhorst, 2025). Misinformation and deep-fakes produced by AI systems are a concern as well as the reality that AI technology is used in war (Ruschemeier, 2025). Most extremely AI has been predicted to enslave humans or contribute to modern-day slavery (Caruana & Borg, 2024).

The rapidly changing and complex nature of AI systems makes it difficult for them to adhere to any legal imperatives of explainability, transparency and equality (Ranchordás, 2021). AI is, however, simultaneously seen as a way to foster innovation and prosperity, thus governments are investing in AI across various industries and its significance in geopolitics is growing (Sloane & Wüllhorst, 2025).

3.2 Issues with AI regulation

AI regulation has recently become a public concern especially with the global market entry of generative AI and the discourse around its risks (Sloane & Wüllhorst, 2025). The rapid advancement of technology has posed some serious challenges to lawmakers and regulatory development. As a result, more experimental approaches, such as regulatory sandboxes and temporary laws, have been developed. (Bagni, 2025; Ruschemeier, 2025.) Due to the dynamic and complex nature of AI there needs to be system of AI governance which includes both general and specific regulations as on specific regulation will most likely not be sufficient (Ufert, 2020).

Issue with regulating AI systems and digital technologies is that they develop and change incredibly fast and developing legislation and regulations is much slower. Insufficient knowledge and uncertainty about what is regulated in the digital world and what is not further complicates regulation. (Ruschemeier, 2025.) Bathaee (2018) argues that strict regulatory frameworks and transparency regulations are inefficient in the context of AI regulation as they have a great risk of prohibiting SMEs and start-ups from entering the AI market and stifling innovation (Bathaee, 2018). Finding the regulatory balance is important because if the regulation is too light essential human rights might be compromised and if it is too strong it could possibly stifle innovation and competitiveness (Caruana & Borg, 2024).

Developers of AI systems have faced multiple major challenges trying to implement and interpret the General Data Protection Regulation (GDPR), more specifically Article 22, regarding individual's rights in the AI environment which includes automated decision-making, explainability of AI decisions and the involved logic, and the data used in developing AI models. The challenges arise from a lack of legal guidance and ethical principles on how to use AI in different areas of society. These challenges are even more prevalent in SMEs as they usually do not have the skills, knowledge, human resources or budget to tackle these issues. (Crockett et al., 2023.)

Regulations are often accused of prohibiting innovation. Experimental regulations, however, are meant to be solutions to this issue. They are supposed to promote innovation and additionally generate knowledge of AI systems in order to further improve and shape the regulatory framework around AI. (Ruschemeier, 2025.)

3.3 Who should be regulated

The main question in AI regulation is who should carry the legal responsibility. In the context of the AI Act, the developer has the knowledge and practical control of the AI system which includes the algorithms and training sets for example. Based on this, it could be stated that the developers are legally responsible especially when they profit from licensing their service or product. However, when discussing general-purpose AI, the responsibility of the provider may exclude the responsibility or liability for unforeseeable risks. It might also be impractical to hold deployers liable for certain occurrences as it can be impossible for them to audit or repair issues of data quality. (Caruana & Borg, 2024.)

Both the public and private sectors, especially SMEs, will have to take responsibility and accountability of the behaviour of their AI systems as the general population becomes more aware of the effects and risks of AI and data privacy. Damage to the public image and reputation can lead to decreased business. From the perspective of business, a relation between the perceived risk of an AI system in a certain context and the amount of trust that users have in its decision-making is prevalent. (Crockett et al., 2023.) The AI Act applies to both private and public actors. These include providers and deployers of AI systems placed in the EU market, who are located in the EU or the output of their AI system is used in the EU, distributors and importers of AI systems, product manufacturers who combine their product with an AI system and affected persons located in the EU. (Caruana & Borg, 2024; EU, 2024.)

3.4 Regulation and SMEs

SMEs face particular challenges regarding AI innovation and integration. Generally, SMEs have limited resources including financial and skilled employees, they also face substantial economic pressure, thus their ability to invest in and adopt new technologies is restricted. The quickly changing regulatory environment furthermore poses challenges to AI innovation. (Wolf-Brenner et al., 2024.) The quickly evolving regulatory landscape and the legal consequences of possible non-compliance are barriers that companies, especially SMEs, face with implementing big data processes. They also face issues with distinguishing personal and non-personal data. (Timan et al., 2021.)

Wolf-Brenner et al. (2024) found in their study that 55% of SMEs in Europe see administrative obligations and regulatory barriers as significant challenges. In their study they interviewed executive representatives from eight Austrian SMEs. They found that within these companies, the

majority used AI systems provided by a third party, only two of them were developing their own AI system. In addition, they discovered that the companies using third-party provided solutions were not as engaged or concerned with AI regulations such as the AI Act which could be result of insufficient understanding of the implications of said regulation. Instead, companies developing their own models were more engaged with regulations such as the AI Act. (Wolf-Brenner et al., 2024.)

4 Artificial intelligence regulations

4.1 AI regulations around the world

In recent years a notable amount of guidance of the ethics of AI and technologies driven by data have been introduced by different corporations, governments and international actors. Legal frameworks regulating AI are also rapidly appearing. Article 22 in the GDPR published in 2018 is considered the first legal approach to governing information in the context of automated decision-making. (Crockett et al., 2023.) The borderless nature of AI and the challenges it poses are leading towards global AI governance frameworks; however, geopolitical interests and distinct political and social values can lead to regulatory fragmentation and increase competition to take control of the global AI market (OECD, 2023).

The most dominant AI regulatory strategies can be divided into three types which are overhauls, novel regulations and omnibus regulations. Overhauls mean updating already existing regulatory frameworks to better account for AI-specific impacts and risks. Novel AI regulations are new regulations focused entirely on AI. Omnibus regulations are universal regulations that are meant to regulate AI itself and not the application of AI or the industry and they usually affect a larger amount of people than the first two. (Sloane & Wüllhorst, 2025.)

Usually, the first step of AI regulation is the overhaul strategy, but it poses challenges on how existing legal frameworks and laws can include the specific risks and impacts of AI as well as mitigate them. Examples of overhauls are the adaptations made to US anti-discrimination legislation such as the proposed addition to the 1945 New Jersey Law Against Discrimination that would recognise discrimination within automated decision making or AI and protect members of protected groups from discrimination taking place in automated decision-making systems in sectors such as insurance, banking and healthcare. (Sloane & Wüllhorst, 2025.)

Novel regulations are exclusively focused on AI and often focus on a particular type of AI technology, specific use or application of AI or AI skills and literacy. Examples of novel AI regulations include different facial recognition technology focused regulations as well as regulations in the field of AI supported autonomous vehicles. (Sloane & Wüllhorst, 2025.)

Omnibus regulations are not sector specific and might include multiple substantive matters. The EU AI Act is an example of an omnibus regulation as well as several regulatory approaches introduced

in the United States such as the proposed Algorithmic Accountability Act of 2022. (Sloane & Wüllhorst, 2025.)

To name a few more of the existing AI regulations, the Beijing AI Principles published by the Beijing Academy of Artificial Intelligence in 2019 that advocates for ethical AI, and in the same year the OECD published five principles for the responsible management of AI. The United States Office of Management and Budget has published Guidance for Regulation of Artificial Intelligence Applications in 2020 and in 2021 the Draft Text of the Recommendation on the Ethics of Artificial Intelligence was introduced by the General Conference of UNESCO which presents a human-centric approach to artificial intelligence. (Crockett et al., 2023; OECD, 2019; UNESCO, 2021; U.S. Government, 2020.) The UK government has issued a general guidance on Understanding Artificial Intelligence Ethics and Safety which applies to actors in the public sector who work with design, production and deployment of artificial intelligence. The guidance requires the actors to take into account the ethical considerations continuously throughout the AI project. (Black & Murray, 2019; U.K. Government, 2019.)

Many AI regulations or policies also feature disclosure requirements which mean that the user must be informed that they are interacting with an AI. Other transparency mandates include inventories, that should provide information on how AI is used as well as the data used to train said AI system, and red teaming which is used to reveal possible weaknesses and vulnerabilities in an AI system, and it is often performed internally and in a controlled environment by engineers who launch attacks on said system. Human-in-the-Loop requirement is also a transparency method, and it signifies that an AI system is supervised by a human and that users are able to receive human interference if they wish. Additionally, assessments that are used to assess systemic risks of an AI system, are methods of transparency. (Sloane & Wüllhorst, 2025.)

4.2 The EU AI Act

EU's approach to tech regulations stems from the concern that companies in the tech industry do not understand what effects technology can have on democratic institutions or people's fundamental rights and thus AI regulation has recently become a political priority in the EU. The main objective of regulation is to ensure that AI is developed responsibly and with a human-centric approach. (Bradford, 2024; Pošćić & Martinović, 2022.) The goal of European policy and legislative efforts is to establish an AI environment that permits businesses, citizens and public actors to benefit from AI (Ranchordás, 2021). The EU AI Act is the first comprehensive legal framework for regulating AI in the world. Its aim is to make sure that transparency, safety and fundamental rights are taken into

account in the development of AI systems and that said systems are designed with a human-centric approach. Additionally, the AI Act intends to create an environment that does not hinder or stifle innovation. (Caruana & Borg, 2024.) Both the OECD and UNESCO have highlighted the importance of non-discrimination, fairness and equality as well as further endorsed explainability and transparency of AI systems. They have also highlighted the relevance of human intervention and supervision of automated systems to reduce some of the risks of automation to democratic values and human rights. (Moraes, 2024; OECD, 2019; UNESCO, 2022.)

The AI Act applies to any entity that intends to release or already has an AI system available within the EU market regardless of the location of said entity or if they are a public or a private actor (Caruana & Borg, 2024). The Article 3 of the AI Act defines an AI system as a "machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (EU, 2024).

The AI Act categorises AI systems based on their potential risk into four categories: unacceptable risk, high-risk, limited risk and minimal risk AI systems (EU AI Act High Level Summary). The AI Act presents eight types of AI systems that present an unacceptable risk and are thus prohibited. These systems involve manipulation, social scoring, exploiting individual's vulnerabilities, biometric categorisation systems and real-time remote biometric identification (RBI), assessment of the risk of an individual committing a crime, compilation of facial recognition databases by untargeted scraping of data and inferring emotions in educational institutions and workplaces. (Caruana & Borg, 2024; EU AI Act High Level Summary.)

An AI system is classified as high-risk in the AI Act if the intended use of the system is a safety component of a product or the system itself is a product covered by a particular Union harmonisation legislation listed in Annex I of the AI Act and the AI system is required to undergo a conformity assessment by a third party before it can be put into service or placed on the market according to the Union harmonisation legislation. An AI system is also categorised as high-risk if it is referred in the Annex III of the AI Act, such as systems that use biometrics, are used in critical infrastructure, educational training or democratic and judicial processes. (Caruana & Borg, 2024; EU, 2024.)

Limited risk AI systems are systems that do not lead to a significant risk because they do not essentially influence decision-making or pose substantial harm. These systems could be intended to

only perform a small task such as a system designed to delete duplicates among data, enhance the result of a priorly completed human activity, detect decision-making patterns in human completed decision-making processes without intending to replace or influence them, perform a preparatory task to an assessment that is relevant for the AI systems, listed in an annex to the AI Act, purposes. (EU, 2024.) These limited risk systems should follow lighter transparency obligations. Users should be made aware that the system they are interacting with is an AI system. These systems include for example chatbots. Minimal risk AI systems are not subjects to regulation in the AI Act. (EU AI Act High Level Summary.)

Providers of AI systems must comply with the transparency obligations as in they must ensure that users are aware that they are interacting with AI. Additionally, AI generated content must be recognisable as AI generated or manipulated. However, systems that are authorised by law do not have to comply with these obligations. (Caruana & Borg, 2024.)

The AI Act also separately defines general-purpose AI (GPAI) models as AI models that show notable generality and are able to execute a wide range of different tasks regardless of how it is placed on the market and that have the ability to be integrated into various downstream applications and systems. GPAI system in turn is an AI system that is based on a GPAI model and is able to be used for multiple purposes and it might be integrated into a high-risk AI system. (EU AI Act High Level Summary.)

According to the AI Act all providers of GPAI models have to draw up relevant technical documentation, sufficient documentation and information to supply to the providers downstream so that they understand limitations and capabilities, form a policy to comply with the Copyright Directive and publicly provide an adequately detailed summary of the content used for the model's training. However, providers of free and open licensed GPAI models only have to comply with the two final obligations except if the model is systemic. (Caruana & Borg, 2024; EU AI Act High Level Summary.)

The risk-based approach of the AI Act essentially means that the amount of regulation a provider or a deployer of an AI system is subjected to depends on how the risk of the system is categorised. Risks to safety, health and fundamental rights are the main concerns in the regulation. (Ho & Caals, 2024.) A considerable portion of the regulatory framework is directed towards high-risk AI systems focusing on their intended purpose and taking into consideration the generally acknowledged state of the art on AI and technologies related to it. (EU, 2024; Ho & Caals, 2024).

The AI Act introduces “ex-ante” and “ex-post” mitigation and testing methods for AI systems depending on which risk category they are assigned to. These methods include for instance audits which can be found in many other AI regulations as well. They are generally comparations between nominal information and values to their actual counterparts and they are designed to identify law of policy violations. (Sloane & Wüllhorst, 2025.)

One of the goals of the Act is to establish an environment of trust in the context of AI to facilitate and support AI innovation and development (Ho & Caals, 2024). As stated in the AI Act in Recital 25, it is supposed to respect freedom of science as well as support innovation and research and development activities. Consequently, the regulation will not be applied to AI systems being tested, researched or developed or to AI models before they are being put into service or placed on the market. (EU, 2024.) If an AI system is meant to advance public interest, personal data collected for distinct purposes could be used for the development of the system, however, only under specific conditions and safeguards in the regulatory sandbox (EU, 2024; Ho & Caals, 2024).

Important EU values such as protecting the environment, human health and safety together with the principle of democracy and fundamental rights are also underlined in the AI Act. The Act presents regulatory instruments such as mechanisms to guarantee transparency, robustness, cybersecurity and human-centredness to mitigate the risks to the values mentioned. The Act also adopts a collaborative approach and encourages the involvement of a wide range of stakeholders to support equality, diversity and equal access and avoid harmful features such as unfair biases and discrimination throughout the entire AI value chain. (Ho & Caals, 2024.) Furthermore, the Act defines AI system similarly to other international organisations to facilitate international cooperation (EU, 2024; Ho & Caals, 2024).

The AI Act has also faced criticism. In article 60 it is stated that high-risk AI systems can be tested outside the sandbox in real-world conditions, but the Act does not specify what these real-world conditions ought to be. In addition, testing AI systems outside the sandbox reduces the possibility of regulatory learning and thus does not fully contribute to developing new legislation. It is also possible to test the AI system under real-world conditions in a sandbox, as stated in Article 76, which further complicates the separation between the two procedures. This allows that in complicated cases the firms will choose the easier option without the sandbox and the possibility of any regulatory learning is lost. (Ruschemeier, 2025.) The Act has also faced criticism from many influential companies in Europe such as Renault and Siemens as they state that the Act could have

negative impacts on competitiveness and investment. Other actors have also raised concerns on the regulation's effect on innovation. (Moraes, 2024.)

There has been discussion around the effects of regulation on innovation long before AI. A social control dilemma, presented in the 1980s by David Collingridge, states that technology should be regulated in a way that harmful social consequences are avoided. In order to achieve this the regulation needs to allow technological innovation without letting the technology become impossible to regulate. One possible solution presented to this dilemma is the regulatory sandbox that encourages the discussion and learning between regulators and developers of new technologies and allows for testing of new innovations in a controlled environment. Additionally, the regulatory sandbox encourages multistakeholderism in AI development. (Moraes, 2024.)

5 The regulatory sandbox

5.1 What is a regulatory sandbox

Whenever a new and unfamiliar technology is introduced, it always brings risks, uncertainties and is often disruptive and consequently, creates regulatory challenges. Innovation and new technologies usually do not go well with traditional regulatory frameworks and regulation often lags behind technological advancements. (Moses, 2011; Moses,2013; Ranchordás, 2021.)

In computer science the term sandbox is used to describe a quarantined or isolated area where the effects do not affect the infrastructure or critical networks on which they run. Regulatory sandbox is somewhat similar to this. Sandboxes can create a so-called safe space for experimentation of new business ideas and thus promote innovation. However, the regulatory sandbox is supposed to generate possibly unknown consequences and external real-world effects for inspection. They're meant for testing of technologies that aren't fully compliant with existing regulations, or the compliance isn't clear. Thus, they are supposed to promote innovation and aid in the development of regulations simultaneously. (Ruschemeier, 2025.)

Regulatory sandboxes are temporal testing programmes for entrepreneurs to test their innovations under the supervision of an authority. Some regulatory sandboxes might involve lightened regulatory responsibilities; however, participants would still need to adhere to tailored safeguards for society. (The Future Society, 2022.) In recent years regulatory sandboxes have been introduced as experimental regulatory tools in EU's newly developed regulatory frameworks such as the EU AI Act and the Cyber Resilience Act (Bagni, 2025). Regulatory sandboxes are proposed as a solution to mitigate the riskiness of regulation persistently being outdated even before it is put into effect. However, their effects on systems that involve an information deficit is unclear, but they could play a role in reducing this deficit. (Ruschemeier, 2025.)

A regulatory sandbox can provide valuable information to regulators on how to regulate new types of products and services by cooperating with private entities and learning from them. This learning poses only minimal risks as the number of participants is limited and only the selected applicants operate under lighter regulations. (Ranchordás, 2021.) The evaluation of whether a legal framework is appropriate for an institution can also be facilitated with the use of a sandbox. Information obtained from a sandbox can considerably save time when an institution is assessing the need to adapt to a certain legal framework. (OECD, 2023.)

Regulatory sandboxes can offer benefits to multiple stakeholders including regulators, firms and consumers. Benefits to regulators can be promoted engagement and communication with market participants, information gained by learning and experimentation to use in long-term policy making, removing regulatory barriers to beneficial innovation and signalling commitment to learning and innovation. To firms the sandbox can offer reduced time to market and regulatory uncertainty, feedback on regulatory risks and requirements as well as remove market entry barriers which is especially important for SMEs and start-ups. To consumers the sandbox can offer greater access to financial goods and introduce new and possibly safer products. (OECD, 2023.)

The benefits of sandboxes include the ability to test innovations under real world conditions which gives more reliable test results and more precise conformity assessment. On the contrary, testing under real world conditions has the potential to exacerbate the risks to third parties and users if for example real personal data is used. Consequently, this requires the implementation of proper safeguards and the supervision of a suitable authority. (Bagni, 2025.) A regulatory sandbox promotes innovation by allowing the experimentation and exploration of new innovative technologies and products under supervision. When properly used, the regulatory sandbox could be beneficial for all stakeholders, it allows innovators to test their innovations in a supervised and controlled environment, and it helps regulators to understand the technology. Yet, a sufficient legal framework is needed to prevent the misuse of the sandbox. (Caruana & Borg, 2024.)

During the implementation of ethical values into an AI system it is almost necessary to involve experts from different fields in the process (Moraes, 2024). According to the OECD during the development and use of the AI regulatory sandboxes there should be sufficient technical knowledge to prevent misleading results that can lead to major risks to individuals and society as well as negative economic effects (Moraes, 2024; OECD, 2023). The knowledge gaps between different actors related to AI such as regulators and developers are also a challenge. Making AI ethical requires multistakeholderism, different perspectives and experiences of different actors and communities affected by AI need to be heard in the discussion around regulating AI. (Moraes, 2024.)

The regulatory sandbox allows innovators, regulators and other stakeholders to learn from each other and experiment how new ideas and innovations can be modified to better adhere to the necessary regulations. AI regulatory sandboxes have the potential to be used to integrate ethical values into the development process of an AI system as they provide an environment where it is possible to experiment with the potential implementation of these values. (Moraes, 2024.)

There are different types of sandboxes to fulfil different obligations. In regard to the participants, there are private industry specific sandboxes for specific types of technology, public sandboxes for public operators in the context of public procurement and hybrid sandboxes that would be open to both public and private actors. Sandboxes can also be divided into categories by their intended results. For example, there are law-specific sandboxes that are used to gain knowledge on how to potentially modify a specific legislation or regulatory framework by testing technological applications' effects on them. Technology-based sandboxes are meant to test specific technologies in the context of different legislations. Generic and cross-sectoral sandboxes include different types of sandboxes to test several types of technologies. There are also government technology or regulatory technology sandboxes that are used for the process of public procurement. (OECD, 2023.)

According to the report by The Future Society (2022), sandboxes have several primary and secondary functions that they should achieve. Primary functions of sandboxes include "providing monitored regulatory flexibility for entrepreneurs to "live" test their innovations on the market", "providing regulators with a greater understanding of the cutting-edge technologies, value chains, and business models" and "providing customers (B2B or B2C) with the confidence to do business with disruptive technology providers". In addition to the primary functions above the EU AI Act sandbox could provide secondary functions depending on its intentions and design. These could include lowering market-entry barriers, providing entrepreneurs with a central solution to address regulatory doubts and ambiguities, improving the regulatory frameworks as the regulators gain knowledge of their own regulatory tools, providing end-to-end support for all applicants, and attracting global applicants to the European AI sandboxes and thus help unify the international landscape on AI regulation. (The Future Society, 2022.)

Based on the distinction between AI systems integrated into products and services and sole AI systems, The Future Society recommends two different types of regulatory sandboxes to be developed. The first is a physical regulatory sandbox for tangible products and services that contain AI systems such as autonomous vehicles and smart medical devices. The AI system embedded is dependent on some physical trait, for instance a hardware. The second type is a cyber regulatory sandbox for AI systems that operate in the cyber environment and do not depend on any physical context. For example, chatbots and several types of algorithms are such AI systems. The two types of regulatory sandboxes require very different levels of resources which makes the distinction between them important from a cost-effectiveness perspective. (The Future Society, 2022.)

The Future Society offers a recommendation for developing the EU AI regulatory sandbox that includes three phases. Ideally, the first phase would be creating the demand for AI regulatory sandboxes which would be achieved by informing the different stakeholders of the benefits of a sandbox such as increased knowledge for both regulators and entrepreneurs. This would require establishing an innovation hub which allows entrepreneurs and regulators to establish connections and achieve joint understanding. The sandboxing system would be centralised at the EU level and the EU would cooperate with national authorities to avoid fragmentation of the Digital Single Market and regulation. (The Future Society, 2022.)

The second phase involves allowing the regulators and society at large to fully understand the value that a regulatory sandbox can bring. This would be achieved by clear informing and providing evidence to the customers and other stakeholders of newly developed AI systems. It should also be ensured that regulators have the competence and correct equipment to ensure the safety of sandbox participants' customers. (The Future Society, 2022.)

The final phase would consist of reviewing, evaluating and improving the sandbox ecosystem based on the generated information. Based on the information obtained through the review, relevant authorities would conduct a plan for more efficient opening of sandboxes and scale the entire ecosystem to allow for larger impact. Again, the distinction between physical and cyber sandboxes is important as opening a physical sandbox is much more demanding and costly than a cyber sandbox. (The Future Society, 2022.)

Typically, regulatory sandboxes share key features such as utilising a trial-and-error approach, being temporary and involving multiple stakeholders. They need to be designed in a way that does not result in inaccurate outcomes that can have negative effects on consumers, competition, data protection and regulation. (OECD, 2023.)

The process of a sandbox incorporates first an application phase then a preparation phase followed by a testing phase and finally and exit and evaluation phase. Entry to a sandbox can be granted through different criteria such as innovativeness and ideally the entering stakeholder would benefit from cooperating with a relevant institution. (OECD, 2023.) First a certain authority or agency allows applications for a sandbox to be submitted from companies that have a product ready for testing followed by the selection of sandbox participants based on predetermined criteria. Then selected companies will enter the testing phase where their product is tested in the market under the administration of a relevant authority for a certain time period. Finally, upon exiting the sandbox the tested product is either pulled from the market due to non-compliance or launched to the public

market. (The Future Society, 2022.) The applicable regulations during the testing phase of the sandbox should be clearly defined before the testing begins to guarantee legal predictability. To ensure this, there needs to be clear and established rules for entry and exit, included areas and applicable legislation need to be specified, clear time frame for the sandbox needs to be established and proper safeguards need to be put in place to reduce the possibility of risks. (Bagni, 2025.)

These phases can be seen in the financial technology (fintech) sandboxes as well. The usual regulatory sandbox process consists of several phases. First, the application phase where companies submit their application to the responsible authority, typically in an application period that lasts up to two months. The competent authority then assesses how well the application fulfils the selection criteria. These selection criteria are transparent and available to the public. Next is the preparation phase where the competent authority determines the plan and the framework for testing including defining the parameters for testing, finding out if the tested proposition involves any regulated activity, operational needs and any needed disclosures to the relevant customers. (ESMA, EBA, EIOPA, 2018.)

Then comes the actual testing phase where the proposition is tested in the sandbox. These phases can last several months and depending on the authority, usually this phase lasts for 6–12 months. During the testing phase, the company should communicate with the competent authority. The authority could issue a warning or terminate the test completely if the company does not adhere to the agreed parameters. (ESMA, EBA, EIOPA, 2018.) Reporting is a key feature of the sandbox as it provides important feedback to the sandbox administrators and is thus a major aid in developing and modifying regulation. Reporting should be required even after exiting the sandbox and during operating on the open market. (Ahern, 2021.)

Finally, after the test phase, the project is evaluated. Typically, either the company submits the required final report to the authority, or the authority will evaluate the test. (ESMA, EBA, EIOPA, 2018.) Planning a proper exit strategy is very important for the companies entering a sandbox. Properly entering the open market from a controlled environment of the sandbox is very important to ensure consumer protection especially in the fintech context. Recognising that the tested product or service may not pass the testing phase is also necessary. (Ahern, 2021.)

Designing a sandbox usually includes several key features such as resource allocation, often the successful administration of a sandbox calls for a notable amount of human resources, deciding the appropriate time limit, determining if the participants upon exit can be immune to certain regulatory obligations and developing safeguarding measures to ensure that the immunity does not pose a risk

to adhering to regulatory objectives and determining the intensity of regulatory supervision to promote the proper design and enforcement of these safeguards. Selection criteria such as if the product is new enough and which level of market-readiness it has are also important design features as are the anticipated benefits to society and consumers, the theme of the sandbox, for example AI, and the number of participants. (The Future Society, 2022.)

The design and management of the sandbox greatly affect and determine if the sandbox produces effective results for various stakeholders such as entrepreneurs, regulators and society. The resource-demanding nature of the sandbox also means that the assessment of return to investment need to be taken into careful consideration. (The Future Society, 2022.) How the sandbox is designed could have major impacts on markets and competition. For example, if not carefully assessed prior to implementation the use of the sandbox could result in unfair competition. (OECD, 2023.) Often regulatory sandboxes have safeguards and mechanisms to mitigate the risk of any negative consequences. These safeguards often are often linked to consumer protection, data governance and safety and they can be such as limiting the number of customers, close monitoring, reporting obligations, risk mitigation and specifying the regulatory waivers in the sandbox. (Attrey et al., 2020.)

Often only a small percentage of applicants are selected into a sandbox based on predetermined eligibility criteria such as innovativeness. How innovativeness is defined is an important thing to consider. Patents could be utilised when defining innovativeness, however, there are risks of the patented technology becoming essential as the sandboxing process has excluded potential competitors due to the lack of a patent. (OECD, 2023.) Additional selection criteria may include test-readiness and demonstration of consumer benefit. Applying companies are in some cases also required to show how their idea would benefit consumers such as offering higher quality products and services or lower prices. In some cases, they may also be asked to demonstrate social benefits such as inclusivity. Moreover, applicants are often required to demonstrate that their product development stage is ready for sandbox testing and that they need the lightened regulatory environment offered by the sandbox. (Attrey et al., 2020.)

To ensure efficient decision making regarding the access to a regulatory sandbox, technical expertise on emerging technologies should be considered as the authorities responsible for the sandbox might have insufficient knowledge about the technicalities of certain AI systems. This would benefit the markets as well. Liability regimes in sandboxes are important as well, as inefficient regimes could result in reluctancy of companies to take part in a sandbox as they do not

want their algorithms and trade secrets to be exposed to a sandbox with inefficient liability regime. This could negatively impact both innovation and competition. (OECD, 2023.)

A cross-border AI framework has the potential to improve new companies' access to global markets and improve regulatory certainty. Such a framework would allow sharing of practices, cross-border sandbox frameworks and help generalise the terminology and standards around AI and regulatory sandboxes. This could, nonetheless, be difficult due to challenges such as different understandings of risk and varying complex legal frameworks. To encourage cross-border sandbox compatibility the eligibility criteria such as innovativeness should be globally agreed upon as the differences in definitions and interpretations could result in AI companies having to go through several sandboxes and receive different testing result and access decisions. (OECD, 2023.)

As regulatory sandboxes are still developing tools there are different ways of implementing them. In the financial sector, for instance, the aim is often to test and uncover the benefits of a new system and to reduce regulatory entry barriers. This can be achieved by temporary suspension of rules. (Moraes, 2024.)

5.2 Regulatory sandbox under the AI Act

Concerns of strict regulation negatively impacting future development in Europe have been brought up for years. Solution to this could be the regulatory sandbox presented in the EU AI Regulation Proposal (later the EU AI Act). Regulatory sandboxes as well as other experimental regulations are supported for multiple reasons. Tools of experimental regulation allow innovators to experiment without the burden of strict regulatory frameworks. (Ranchordás, 2021.) The EU AI Act introduces regulatory sandboxes as ways to support innovation and demands that SMEs and start-ups are granted a priority access to these sandboxes and are offered education on new regulations as well as advice through designated communication channels (Caruana & Borg, 2024; EU, 2024). One of the goals of the regulatory sandbox is to facilitate market entry for SMEs and start-ups by not only fostering innovation but also removing barriers (EU, 2024).

The EU AI Act requires that each member state establishes at least one AI regulatory sandbox at a national level either alone or together with other member states to facilitate development, innovation as well as identify and mitigate risks of AI systems prior to their release to the market. Additionally, the regulatory sandbox should contribute to regulatory learning for authorities. (EU, 2024; Ho & Caals, 2024.) The AI Act also requires complete documentation of the entire sandbox

journey to verify testing process and achieved results (Bagni, 2025). Furthermore, it requires that each member state sets up a framework for supervision and governance (Caruana & Borg, 2024).

The main objectives of the AI Act regulatory sandbox are 1) bettering the legal certainty in order to comply with the provisions of the AI Act or other relevant national or Union legislation, 2) supporting collaboration and exchange of knowledge between authorities and other stakeholders, 3) promoting innovation, competitiveness and the advancement of an AI ecosystem, 4) increasing the regulatory knowledge of AI system providers and 5) providing SMEs and start-ups with better premises to enter the Union market (Bagni, 2025; EU, 2024). It is stated in the AI Act that the aim of the regulatory sandbox is to improve legal compliance with the Act itself and other applicable legislation, foster innovation as well as contribute to regulatory learning. The regulatory sandbox is also supposed to help SMEs and start-ups to access the Union market. (Ruschemeier, 2025.)

According to the AI Act, AI regulatory sandboxes could also help mitigate risks related to privacy. Existing privacy sandboxes concentrate on themes such as privacy-by-design approaches, risks associated with new technologies and how to assess and mitigate them and international data flows that call for international regulations. A sandbox for privacy could also involve other regulations besides privacy and an AI sandbox could simultaneously consider privacy regulations due to the multisectoral nature of AI applications. (OECD, 2023.)

Additionally, the Act encourages cooperation between AI developers, academics and experts on non-discrimination, inequality and accessibility as well as experts on environmental, consumer and digital rights to make sure that the outcomes of AI are environmentally and socially beneficial. According to the Recital 143 of the AI Act, interests of SMEs and start-ups should be taken into a particular account to encourage and promote innovation. This is why SMEs in particular should be granted a priority access to these AI regulatory sandboxes. (EU, 2024.)

The anticipated challenges and solutions of AI regulatory sandboxes include collaboration between stakeholders such as relevant authorities, companies and data protection authorities, technical knowledge of regulatory authorities, need for stronger international collaboration, developing a harmonised eligibility and testing criteria to decrease the amount of regulatory fragmentation, taking the effects of innovation and competition into special account and considering how regulatory sandboxes could be combined with other regulatory mechanisms (OECD, 2023).

AI providers, including SMEs and start-ups, have reported that in their opinion a sandbox environment could aid in the development and innovation of more responsible AI. They would be

interested in participating in a sandbox to test their AI systems in real-life conditions. Studies have shown that experimental regulatory tools, such as regulatory sandboxes, have helped SMEs and start-ups reduce their compliance costs by receiving technical and legal assistance. They also have the potential to reduce unforeseen risks and consequences. If a company has participated in a sandbox, it can also attract investment and strengthen their position in the market. (Zarra, 2025.)

There are, however, some criticism regarding the sandbox proposal in the AI Act. The regulatory sandbox does not adequately balance the innovative experience and liability protection. This could lead to limiting innovation and create a fabricated sense of compliance and safety in the market. (Truby et al., 2021.) They have also faced criticism regarding their design and methodology. For instance, if the sandbox is designed inefficiently and the assessment criteria is inadequate, potential risks might go unnoticed. (Ranchordás, 2021.)

5.3 Regulatory sandboxes around the world

The US Consumer Financial Protection Bureau (CFPB) developed the first sandbox-style framework in 2012 and even though it was not formally announced as a sandbox, it exhibited many features of a sandbox. The goal was to support the development of innovative financial products and services that would be accessible to consumers. The project involved collaboration with the innovator community to reach the goal. (Ruschemeier, 2025.)

In recent years the use of regulatory sandboxes has grown more popular (Moraes, 2024). The field of fintech, due to its characteristics of sector-specific regulatory supervision and being highly technical, was among the first fields to try the sandbox approach (Bagni, 2025). The first implementation of the regulatory sandbox is by the UK's Financial Conduct Authority (FCA) in the year 2016 (Moraes, 2024; Ruschemeier, 2025). The FCA sandbox takes a market-driven approach and includes AI related innovations in the context of the financial sector (OECD, 2023; Ruschemeier, 2025). Since the introduction of the FCA regulatory sandbox, many other entities have developed a sandbox of their own. These sandboxes can be found in a wide variety of different sectors such as data protection, financial and health. (Moraes, 2024.) These sandboxes can be found in Hong Kong, Australia, Canada, Abu Dhabi, Kenya, Thailand, Malaysia and Singapore among others (Buckley et al., 2020; World Bank, 2020).

Another field where the sandbox experiment has been adopted is the processing of personal data. For instance, Norway and the UK have their own sandboxes in this field. The Information Commissioner's Office (ICO) is responsible for the UK's sandbox which focuses on technologies

such as facial recognition and biometrics. Additionally, it offers support on integrating data protection and risk mitigation to companies free of charge. (Bagni, 2025.)

The ICO sandbox incorporates AI systems related to privacy and offers new interpretations of privacy related regulations to better be applied to AI systems, and its main goal is to support organisations that incorporate and use personal data in their products and services (BIAC, 2020; OECD, 2023). Experiments from this sandbox show that the privacy sandbox can support open communication between stakeholders and help recognise risks and regulatory uncertainties (BIAC, 2020). Other benefits include increased compliance confidence regarding the developed products and services, increased understanding of data protection frameworks, increased trust as the participant has demonstrated an interest in data protection and promoting the development of products and services that bring value to the consumer (Truby et al., 2021).

With the example of the UKs ICO sandbox, Norway also initiated their own regulatory sandbox administrated by the Norwegian Data Protection Authority (Datatilsynet) which aims to help participants develop innovative products that are privacy-friendly, ethical and compliant to the data protection law (Olsen, 2020). The sandbox requires participants to comply with the Personal Data Act but exempts them from any enforcement action during the development process (OECD, 2023). The sandbox project introduced in 2020 focuses on innovation in the context of privacy. Participants of this sandbox have been very diverse, from the fields of environment, health, transport and digital services, both public and private actors have been selected. It has also included generative AI products and services. Until the year 2023 total of 12 applicants have been selected and tested in the sandbox. The selection process of the Norwegian sandbox has been thoroughly documented, and the project has been evaluated. The transparent and comprehensive documentation of the project encourages responsible and ethical application and sufficient supervision by an authority. The guidelines of the sandbox were based on the ethics guidelines for trustworthy AI by the High-Level Expert Group on AI by the EC. (Ruschemeier, 2025.)

The French sandbox administrated by the National Data Protection Commission (CNIL) includes projects from the health sector. The sandbox offers support to participants on how to implement privacy into their development process from the beginning. The sandbox requires participants to comply with the GDPR (OECD, 2023.) Currently the sandbox only provides technical and legal support (Ruschemeier, 2025).

The Monetary Authority of Singapore (MAS) operates a fintech regulatory sandbox that includes testing of AI products with the aim of strengthening internal administration of AI applications and

promote data management in the financial sector. They released the Fairness, Ethics, Accountability and Transparency (FEAT) principles to promote the use of these values in regard to AI and data analytics. MAS collaborated with different stakeholders from the financial industry to develop the FEAT principles. (OECD, 2023.)

In Korea the Ministry of Trade, Industry and Energy, Ministry of Science and ICT and the Ministry of SMEs and Start-ups collaborated to introduce a sandbox that allows participants to test their innovations and innovative business models without regulatory burdens for a specified amount of time (OECD, 2021; OECD, 2023).

The Australian sandbox administrated by ASIC allows the selected participants to operate in the sandbox without the Australian financial services licence that is otherwise required. However, the participation has been limited due to the eligibility criteria and restrictive conditions subjected to this waiver. (Buckley et al., 2020.)

The Federal Ministry of Economics and Technology (BMWi) in Germany has introduced the Real-World Laboratory Act concept with the aim of reinforcing Germany's economical position by promoting innovation and making Germany attractive to companies. Discussed potential areas of operation would be for example digital legal assistance, digital identification innovations and AI applications. Up to this point sufficient legal standards haven't been established. (Ruschemeier, 2025.) The goal of this experimentation would be to facilitate the AI adoption of firms and provide the government with valuable information to potentially modify existing regulations. Germany's office for Regulatory Sandboxes at the Federal Ministry for Economic Affairs and Climate Action plans to introduce experimentation clauses as basis for regulatory sandboxes, establish a regulatory sandbox network, coordinate a contest of regulatory sandboxes and give a Handbook for Regulatory Sandboxes in order to promote regulatory experimentation. (Bagni, 2025; BMWi, 2019; OECD, 2023.)

Other sandbox approaches have also been introduced. Estonia's sandbox approach aims to facilitate the collaboration between the private and public sectors in the development of IT. Estonia's approach also supports the quicker implementation of AI solutions. Lithuania has plans to establish a regulatory sandbox that could be used in the public sector to test AI systems. Malta and Colombia also have established regulatory sandboxes that focus on emerging technologies (Malta) and privacy-by-design (Colombia). (OECD, 2023.)

The first AI regulatory sandbox linked to the EU AI Act was initiated in Spain in 2022 and is done in collaboration with the European Commission. The sandbox aims to test the AI Act with actual AI applications to evaluate effects on regulation and development of said applications. Specific goals of the pilot project include clarifying the regulations and requirements posed on to AI systems, providing information on how to comply with the regulation and promote development of trustworthy and innovative AI systems, beginning the process of creating a National Supervisory Authority in Spain, aiding in the development of cohesive national and European standards and guidance and support the implementation of the AI Act which is supposed to be put into force in 2025. (OECD, 2023.) The aim of the Spanish sandbox is to investigate the functionality of the AI Act's obligations, and the results are meant to contribute to the identification of best practices and provide technical guidelines for administration and implementation while a typical sandbox would promote collaboration between stakeholders to improve a regulatory framework (Ruschemeier, 2025).

The testing of other experimental regulatory tools will also be conducted in the Spanish sandbox pilot as stated by the EC. These would include Testing and Experimentation Facilities (TEFs) which offer infrastructure, tools and a framework to test innovative AI products, for example their compliance with regulations and AI standards. Additionally, TEFs and AI standards could be included in the testing phase of the sandbox to gain insight into the standardisation process. Preparatory drafts of AI standards could be tested in the sandbox and simultaneously TEFs could provide additional technical aid that is required with particular AI applications. (OECD, 2023.)

Typical characteristics of the existing regulatory sandboxes are for instance the involvement of innovative products and services that are in a testing-ready state, bring additional value to society or consumers and bring financial benefit during the testing period (Bagni, 2025). Selection criteria for all fintech sandboxes are often influenced by the original FCA sandbox model and they are usually more indicative than exhaustive. Most selection criteria focus on innovativeness and market. Additionally, the applying innovation should be ready for testing. This includes not only looking at the product itself but the state of the business such as a business plan, governance structures and personnel including management. Selection criteria should also include a perceived benefit of accessing the sandbox other than free regulatory consultation. (Ahern, 2021.) Defining clear and transparent selection criteria for sandboxes would support the European Commission's Expert Group's on Regulatory Obstacles to Financial Innovation statement that different types of innovators should be able to apply to a sandbox without being discriminated against (Ahern, 2021; European Commission, 2019a).

5.4 Findings from the existing sandboxes

Regulatory lag is evident in fintech, and insufficient and complex regulatory landscape has both competitive and commercial consequences, for instance navigating incorrectly oriented regulations is complex and costly and especially effects start-ups. However, if regulations are developed too fast and are reactive it might hinder innovation. Regulatory sandboxes in the fintech field are designed to recognise innovation and facilitate the understanding of complex regulations to ideally achieve consumer benefit. They allow tech innovators to test experimental products in a controlled environment before fully releasing it to the market. (Ahern, 2021.) Regulatory sandboxes can provide opportunities for companies such as market entry and faster time to market as well as live-market testing (Attrey et al., 2020).

The sandbox approach is used as a regulatory tool in the financial sector to help protect consumers while not hindering economically important innovation since the implementation of the UK's FCA sandbox (OECD, 2023; Zetzsche et al., 2017). Sandboxes are usually able to host only a few participants at a time because of the increased risk to consumer protection that comes with increased number of participants. Despite the small number of participants, the results of the sandbox show that it is useful for the development process of these few participants. Additional benefit of the sandbox is that it indicates to the market operators that a regulator is open to innovation and willing to be flexible. (Buckley et al., 2020.)

The objectives of the fintech regulatory sandboxes can be categorized into two categories that are regulator focused, and participant focused. Regulator focused objectives promote the learning of the regulator and the development of regulation based on the information gained from the participants and the testing. Participant focused objectives promote and aid in the company's market entry and the development of new products and services as well as increase the companies' regulatory knowledge. (Dardykina, 2026.) The benefits and challenges of the fintech and privacy sandboxes are presented from a participant focused point of view as this thesis focuses on SMEs. However, sandboxes provide potential benefits and pose challenges for other actors as well such as regulators and consumers.

5.4.1 Benefits

The experiments done in the fintech field display clear benefits of the regulatory sandbox. These include facilitated market entry and financing, reduced time to market due to lowered transaction and administrative expenses. Regulatory sandboxes also facilitate the correct interpretation of

regulations. (Dardykina, 2026; OECD, 2023.) The privacy sandboxes can also offer many benefits for companies. These benefits are for example a safe space for testing the compliance of their innovations, access to regulatory guidance and reduced regulatory uncertainty, business development opportunities and incentives to innovate as well as accelerated time to market. (BIAC, 2020.)

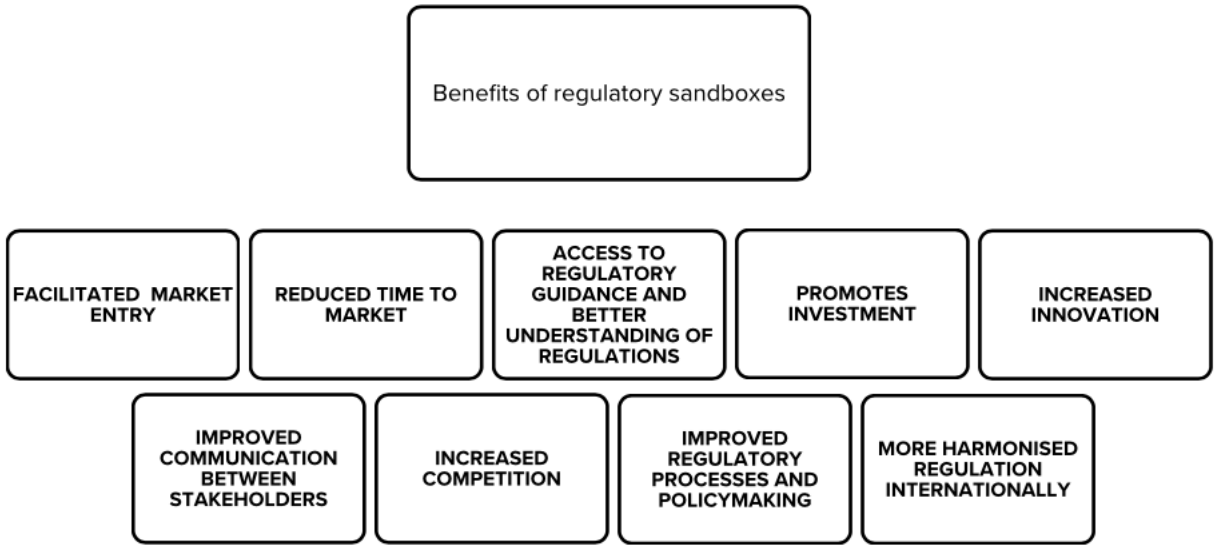

Figure 1. Benefits of regulatory sandboxes

A clear positive effect of the sandbox approach is that it promotes investment in the market, especially investment directed at fintech start-ups. Innovative companies have better access to financing due to the environment that the sandbox provides that allows testing in the market and decreases regulatory uncertainty. For instance, results show that investment in the fintech sector was 6.6 times higher after firms' successful testing in the sandbox. (Goo & Heo, 2020; OECD, 2023.)

The regulatory sandbox facilitates market entry by reducing regulatory barriers to innovation. With regulatory sandboxes the transaction and administration costs are significantly lower. The average speed to market was increased by 40% in over 700 companies that were participating in the UK's FCA sandbox compared to the standard authorisation time of regulators. (OECD, 2023; Truby et al., 2021.)

Sandboxes are also educational for the different stakeholders involved. Policymaking and regulation processes are improved by the communication and learning between regulators and innovators. Regulatory sandbox can also facilitate communication between players from different sectors.

(Attrey et al., 2020; Buckley et al., 2020.) For example, results from the innovation hub and sandbox initiatives administered by the Dutch Authority of Financial Markets (AFM) and Dutch Central Bank (DNB) demonstrate that communication and learning between market operators and regulators is essential for improving the regulatory response to financial innovation (AFM & DNB, 2019; OECD, 2023).

The sandbox approach facilitates companies' interpretation of regulations as participating regulators offer clarifying guidance to the interpretation on regulatory frameworks (OECD, 2023). For regulatory authorities, the regulatory sandbox can offer help in understanding how to facilitate and regulate innovations. Regulators have reported that the sandbox has offered benefits such as increased innovation, increased competition and lowered entry barriers, improved regulatory compliance and supervision and increased operational and cost efficiencies of financial innovation. (World Bank, 2020.)

Sandboxes also contribute to the harmonisation of sector-specific regulations internationally which can be seen in the field of fintech. Additionally, the entry requirements for sandboxes are similar across different countries. (ESMA, EBA, EIOPA,2018; Parenti, 2020.) Most common entry requirements for fintech sandboxes are genuine innovation, consumer benefit and financial system benefit, understanding of the regulatory framework, project maturity and test readiness, need for testing, risk mitigation, serve domestic market and commitment to compliance and investor protection (Parenti, 2020). These entry requirements can be found in regulations of for instance Spain, Brazil, Greece, Austria, UK, Us state of Wyoming and Malta among others (OECD, 2023).

The implementation of a fintech regulatory sandbox demonstrates some clear benefits that include sending a positive message by the regulators to the market, foster innovation and support regulatory learning. Sandboxes, when used together with an innovation hub provide regulators with additional learning opportunities. They change how industry operators view regulators, instead of seeing them as something to be avoided, they are seen as important assistance when it comes to regulatory uncertainty. Fintech sandboxes have been beneficial to both regulators and fintech start-ups as they can have an open discourse without the companies risking their license and regulators can anticipate risks better. (Buckley et al., 2020.)

Results from the regulatory sandbox administrated by Datatilsynet have also been reported and generally, they have been good. Through the sandbox participation, the companies have gained valuable information on their technologies, data protection and user communication. The participants have reported that the sandbox helped them understand their own technologies and the

market better. They have better understanding of how to incorporate regulatory frameworks in their products and services. However, the sandbox could be improved by incorporating more technological expertise and diversifying the communication about the projects. (Datatilsynet, 2023.)

5.4.2 Challenges

The fintech regulatory sandboxes pose certain challenges such as the lack of unified eligibility criteria and experimenting processes. Insufficient design of a sandbox could result in damage to competition, stakeholders and data. (Dardykina, 2026; OECD, 2023.) Without proper assessment before the implementation of a regulatory sandbox, it can pose serious risks to regulation and consumers. There is a risk of insufficient safeguards if innovation is prioritised too much and this poses risks to consumer protection. (Parenti, 2020; OECD, 2023). As much as 25% of regulators initiated sandboxes without properly assessing the collateral impacts or potential outcomes and did not have adequate resources and efforts for the entire sandbox process (OECD, 2023). The balancing of risk mitigation through appropriate regulation and promoting innovation is an additional challenge that carefully needs to be considered when implementing a regulatory sandbox (Dardykina, 2026). Possible risks of untested products can be difficult to predict (Attrey et al., 2020).

There are also concerns regarding the vagueness of the selection criteria for sandboxes and that the evaluation of the eligibility of applicants is too open to interpretation which, if left untreated, can cause sandboxes to be less efficient. For instance, “innovativeness” as a selection criterion is not adequately defined which leads to its subjective interpretation by regulators. (OECD, 2023.) The sandbox poses potential risks such as unfairly allocating resources between regulated and unregulated entities if resources are offered to those participating in the sandbox. However, the time limits of the sandbox decrease that risk. A balance between protecting the financial systems and its clients and the promotion of innovation is important to find. (Buckley et al., 2020.)

The future scalability of sandboxes is also important to consider. Currently, the number of participants in sandboxes is quite low compared to those who could be interested in it. The competitive benefits of sandboxes may increase the market pressure to include more participants at a time as well as the regulators’ desire to collect more informative data from participants. The enlargement of sandboxes would require careful preparation and even the automatization of certain processes. (OECD, 2023.)

The regulatory sandboxes for privacy have some challenges such as unclear regulatory authority and how to successfully guide participants whose innovations are governed by multiple regulatory frameworks. Other challenges include lack of regulatory clarity in the sandbox, uncertainty about how intellectual property interests are protected in the sandbox and potential discrimination, for example smaller companies or companies operating in a certain sector may be excluded. (BIAC, 2020.)

Lack of resources is also a challenge posed by the regulatory sandbox for both regulators and companies. Additional challenges are lack of trust if the rules of the sandbox are not adhered to and the process is not transparent, perceived complexity when several authorities or nations are involved in the process and a lack of harmonization in the sandbox approach. (BIAC, 2020.) There is a need for universal and coherent legal framework regarding sandboxes to avoid regulatory fragmentation. At the time there is not harmonisation regarding the liability systems applicable to regulatory sandboxes and this leads to so-called "forum shopping", where various regulators try to attract participants. Without universal frameworks regulators may lower proper safety standards to attract more innovators and the focus of the sandbox may move away from the evaluation of the tested product or service against the proper regulatory framework. (Dardykina, 2026; OECD, 2023.)

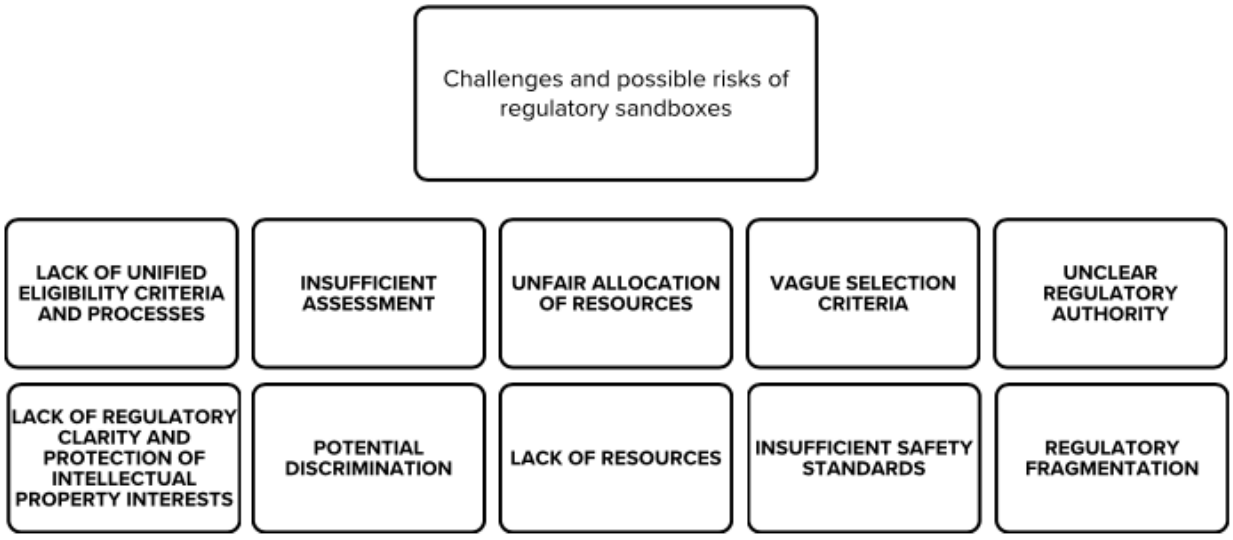

Figure 2. Challenges and risks of regulatory sandboxes

6 Methodology

This chapter explains the empirical methodology of this thesis. The empirical part of this study was done as survey research as there was survey data available to be used in this thesis by the project EUSAiR. This chapter presents the selection of methodology, data collection process, empirical data, data analysis and validity of the results as well as ethical considerations. Respondents of this study were gathered using the self-selection method and the data was analysed using descriptive statistics.

6.1 Selection of methodology

The empirical part of this thesis was conducted as survey research. A survey method was used to gather the attitudes and views of SMEs towards AI development and deployment, AI regulation and the regulatory environment surrounding the practices of these SMEs and the AI regulatory sandbox presented in the AI Act. Surveys are a useful tool for gathering information from large parts of the population and obtaining information about attitudes. However, it is important to note that results obtained from surveys may contain biases that can be caused by lack of responses from respondents or by the accuracy of responses. The respondents may also intentionally misreport their attitudes which also results in errors in the results. (Glasow, 2005.)

The chosen data collection method was questionnaires that included both quantitative and qualitative aspects. Questionnaires can be particularly useful in the information systems field to obtain information of new systems from potential users of said systems. There are several advantages of questionnaires such as collecting large amounts of data for a relatively low cost, they are convenient for the respondent as they are able to answer the questionnaire on their own time, there is no interviewer bias or it is minimal and the data collected through questionnaires is easy to analyse. (Williamsson & Johanson, 2017.)

This thesis was done as a part of the project EUSAiR which is a project supporting the establishment of AI regulatory sandboxes in the EU in alignment with the requirements of the AI Act (EUSAiR, 2024). The two questionnaires that were the data collection method in this study were developed as a part of the EUSAiR project and were not developed by the author of this thesis. The questionnaires were developed to obtain private and public actors' attitudes towards AI development, AI regulation and the AI regulatory sandboxes.

6.2 Data collection

The data was collected through self-administrated questionnaires. Self-administrated questionnaire is appropriate for studies that have a goal of targeting geographically scattered and large population and the data from the participants it to be obtained in relatively short time (Williamsson & Johanson, 2017). For this study the aim was to reach as many respondents in Europe as possible. The questionnaires were available for willing participants on the internet, more specifically the questionnaire of spring 2025 was available for answering in the EUSAiR website. Awareness of the questionnaires was spread through ministries, industry federations and associations and social media. The questionnaire of spring 2025 was available in multiple languages to increase participation and sample size.

As the questionnaires were available through a website this survey study can be classified as an online survey. Online surveys have benefits such as reaching respondents without geographical limits, accommodating any sample size, rapid data collection and they are generally low cost (Williamsson & Johanson, 2017).

To gather the participants a web-based self-selection method was utilised. Self-selection as a sampling method is a form of non-probability sampling which means that the samples have not been scientifically selected, and it is not possible to specify the chance of an individual's inclusion in the sample. Valid generalisations cannot be made when using non-probability sampling so the results of this study can only be applied to the sample. Additionally, the absence of an identified reference population due to self-selection makes it impossible to calculate an approximate coverage or response rate. This also causes the results to concern only the participants. (Keiding & Louis, 2018; Williamsson & Johanson, 2017.)

6.3 Empirical data

As mentioned earlier this thesis was conducted as a part of the EUSAiR project that supports the implementation of AI regulatory sandboxes presented in the AI Act. The project is funded by the EU's Digital Europe program which is a funding program by the EU and the aim of this program is to bring digital technology to citizens, businesses and public administration. The program provides funding for facing challenges related to digital technology. EUSAiR aims to enhance legal and technical capacities, provide standardised frameworks and promote collaboration between EU member states. The project is focused on ensuring that especially SMEs and start-ups among others are able to access the AI regulatory sandboxes. (EUSAiR, 2024; DIGITAL.)

The empirical data for this thesis was gathered through the questionnaires. As mentioned above a self-selection method was utilised which allows different individuals and representatives from various organisations to participate in the questionnaires. The questionnaire of autumn 2024 had a total of 54 respondents of which 31 represented an SME and the questionnaire of spring 2025 had a total of 138 respondents of which 67 represented an SME. In this study only those responses that were from representatives of an SME were analysed as this study is focused on SMEs specifically. These representatives were in different roles in the organisation, the organisations operated in various industries and sectors, and they were located in different countries. The location of the operations also varied. More in-depth description of the demographics is presented in the results chapter.

6.4 Data analysis

The questionnaires were designed in a way that the respondents selected the most suitable answer from given options. Majority of the questionnaire questions were close-ended questions with some open-ended questions where the respondents were able to freely answer the question. The questions regarding the demographics of respondents and the current situations of AI development and deployment in these organisations aimed to provide objective data and the questions regarding the respondents' attitudes towards different aspects of AI development and deployment as well as towards regulation and the regulatory sandbox focused on gathering subjective data.

The questions in the questionnaires were mostly close-ended multiple selection questions where the respondents chose the most suitable answer or answers. There were also a few open-ended questions for the respondents to express their own thoughts that could not be expressed by only answering the close-ended questions. With the close-ended multiple-choice questions there was also an "other, please specify" option which is important in questionnaire design (Williamsson & Johanson, 2017). To gather information on the attitudes of the respondents these questionnaires included multiple questions utilising the Likert scale introduced by Likert in 1932 (Likert, 1932). The questions were organised into related groups. Each question in fully described with the analysis in the results chapter.

Before the data from the questionnaires could be analysed it needed to be prepared first. Data preparation is important to ensure proper analysis, and it involves data cleaning and data transformation and integration (Williamsson & Johanson, 2017). The raw data from the autumn 2024 questionnaire included responses from different sized enterprises and the spring 2025 questionnaire contained data from different sized enterprises as well as public actors and other

irrelevant actors for this thesis. As this thesis only focuses on SMEs, those responses that were not from representatives of SMEs were deleted from the analysed data. The data was also checked for any missing data, errors or duplicates. Any errors in the data such as impossible values or duplicates were not identified. There is, however, no way of knowing if any respondents have selected the wrong option on accident. Any blank values are presented in the results chapter with the full descriptive analysis.

After cleaning the data, the relevant data was transformed into suitable form. The questionnaire of autumn 2024 was already in numerical form except for the open-ended question responses which were coded into numerical form to identify common categories. For all of the open-ended question responses this was not necessary as there were so few answers that it was possible to analyse them without statistical methods. For these cases, common themes were identified. The second questionnaire of spring 2025 was available in two different platforms, Webropol and Typeform and the raw data from Typeform was in written form. The written data was coded into numerical form using the data from the data obtained from the Webropol questionnaire so that the data from both sources could be analysed together.

After data preparation the data was analysed using descriptive statistics. Descriptive statistics are used to describe quantitative data so that it can be interpreted and compared and they involve distribution of data. Distribution of data can be described using central tendency and dispersion depending on the type of data available. Three types of measures most commonly used in measuring the central tendency are mean, mode and median. Dispersion can be measured for example using standard deviation. Data can also be described through graphs. (Williamsson & Johanson, 2017.)

Most of the data of the questionnaires is either nominal or ordinal. Nominal data refers to any measure without order, for example data regarding the demographics of respondents is nominal, and ordinal data refers to data that has order but there are no equal intervals between measurements of score on a scale (Williamsson & Johanson, 2017). Any nominal data was analysed and presented using graphs, tables or stating the distribution. There were also a few questions with the measurement of scale being ratio, that is data that has order, equal measurements on scale and has a true zero point (Williamsson & Johanson, 2017). These questions regarded the technicalities of AI development and deployment in these companies such as time taken in the AI development process and data used in training the AI. These questions do not directly relate to the AI regulatory sandbox

or the research questions of this thesis and are thus analysed only briefly using the mode and the distribution is presented in some of them.

Most of the questions regarding attitudes of respondents towards challenges of AI development and deployment, AI regulation and AI regulatory sandboxes utilised the Likert scale. The Likert scale is considered to be an ordinal scale measure, even though there have been debates around if it can be analysed as an interval scale measure (Huiping & Leung, 2017). Interval scale measures have equal intervals on a scale (Williamsson & Johanson, 2017). In this thesis the Likert scales are treated as ordinal and are analysed as such. Ordinal scales can be described using the median, the middle value of the responses, and mode, the most commonly occurring value (Williamsson & Johanson, 2017). Mean and standard deviation can be used for interval data and thus were not used in the data analysis. Graphical descriptions are useful when presenting the distribution of data (Williamsson & Johanson, 2017). They were used in data analysis to provide a more comprehensive description of the results and to show the distribution of the ordinal data. Any percentages presented in the results are calculated from the full amount of respondents, 31 of the autumn 2024 questionnaire and 67 of the spring 2025 questionnaire.

6.5 Validity and limitations

6.5.1 Validity

The validity of a survey explains how well the survey measures what it is intended to measure. Validity of a survey instrument, in this case the questionnaire, is often measured using four types of tests and these are face validity, content validity, criterion validity and construct validity. Face validity means that the questionnaire is reviewed by non-experts who evaluate whether the questionnaire is comprehensive, clear and appropriate for the target group. Content validity is a formal evaluation conducted experts on the subject and they evaluate whether the content is appropriate and recognise misunderstandings. Both of these tests include qualitative assessments. Criterion validity involves comparing the results of the questionnaire with another test method that is answered by the same respondents or comparing the foresight of the questionnaire with future outcomes. Construct validity is used in retrospective assessment of the questionnaire and measures its performance. (Williamsson & Johanson, 2017.)

Face and content validity were discussed in the kick-off meeting of the project EUSAiR. There were AI regulation experts, legal scholars, technical persons, business and administrative experts as well as non-experts present who evaluated the questionnaires. The first questionnaire was done in

Finland, and it was then compared and improved to an EU-wide version. The comments from the kick-off meeting and issues that emerged during the translation process were also taken into account when developing the EU-wide version. This process fulfils the criterion validity. Construct validity was also taken into consideration as the developers of the questionnaires are very well informed about the contents of the AI Act and how it relates to other regulations and business practices. This allows for the evaluation of responses over time and other actors' opinions, not only enterprises, in the innovation environment are also included.

6.5.2 Limitations

The self-administrated questionnaire has its limitations. Firstly, it is difficult to obtain a sufficient response rate and the self-selection method, due to the absence of an identified reference population, makes it impossible to calculate an approximate coverage or response rate (Keiding & Louis, 2018; Williamsson & Johanson, 2017). Secondly, it is difficult to gather responses from all groups of the population as certain groups are more likely to respond. Additionally, with self-administrated questionnaires the respondents cannot ask for clarification for example when they feel that they do not fit into any of the answer options provided or they do not understand the question and there is a risk of inadequate answer options. During the data analysis, there is also no possibility for the analyser to ask clarifying questions. Furthermore, only simple and easily understandable questions can be asked and there is no opportunity for seeking further information. There is also no possibility to observe the respondents' behaviour and non-verbal communication, and the researcher cannot control how the questionnaire is answered or know if the respondents have provided serious answers. (Williamsson & Johanson, 2017.)

The self-sampling method also has limitations. As it is a form of non-probability sampling, the degree of sampling error cannot be determined meaning it is not known if the sample represents the entire population and to what extent. Calculating the response rate is also not possible utilising the self-selection method, thus the non-response error cannot be determined. Additionally, there is a possibility that the respondents have provided inaccurate data due to misinterpretation or on purpose to present themselves in a certain way and this causes measurement error. (Keiding & Louis, 2018; Williamsson & Johanson, 2017.)

6.6 Ethics

Ethics of a research are important to consider when conducting research. Survey research ethics include obtaining informed consent from the participants, ensuring that there is no harm done to the

participants, minimised deception, protecting the confidentiality of respondents (Oldendick, 2012). The participation to the questionnaires was voluntary as the self-sampling method was utilised, the questions in the questionnaires and the participation were not harmful and the confidentiality of the participants is protected in this thesis.

Ethical survey practice includes transparent reporting of the results, and any methods used in the research as well as conclusions should be entirely disclosed to ensure that the study can be replicated and evaluated. Ethical presentation results means that findings and conclusions made based on the findings accurately represent the information provided by participants. This can be ensured by using statistical methods that are suitable for the type of data during the analysis. (Oldendick, 2012.) Each question in the questionnaires and how it was answered is described and presented in the Results-chapter except for those questions that contained personal data. In the questionnaire of spring 2025 the participants were able to provide their contact information in case they wished to stay updated or contribute to the design of an EU Framework for AI Regulatory Sandboxes. Any personal data was not used in this thesis to ensure that this thesis protects the anonymity of the respondents.

The data from the questionnaires was received from the EUSAiR project and it is stored in an Excel file. There is a copy of the original unedited raw data in one file and another file was made to conduct the data analysis process. More in-depth description of how the data was managed can be found in the research data management plan for students in the appendices.

7 Results

In this chapter the results of the questionnaires are presented using descriptive statistics. First the background of the respondents is presented, then the general use of AI in these companies and after that the respondents' attitudes towards AI regulation are presented. Following that the AI development and deployment and the challenges related to that are presented and lastly, the results from the questions regarding the AI regulatory sandbox are presented.

7.1 Background

In the first parts of both questionnaires the respondents were asked about their background. In the first questionnaire from autumn 2024 the respondents were asked their language, size of the company they represent, in which sector does the company operate, what is their organisation's role regarding artificial intelligence systems and what is their role in the organisation. 30 respondents reported their language to be Finnish and one English. The representation of micro-, small- and medium-sized companies was very equal. 10 respondents represented a micro-sized company, 11 a small-sized company and 10 a medium-sized company. Most of the companies (26%) operate in information and communication field, 10% in wholesale and retail, 16% in other service activities and 16% answered other. Most of the companies reported that their role regarding AI systems was either a deployer (12) or a provider and a deployer (9). Other roles that these companies had were importer, distributor, authorized representative, developer and consulting. Most of the respondents reported to be the company's top management (48%), 32% reported being specialists and the rest were middle management, entrepreneur and future owner.

Demographics			
		Number	Percentage
Language	Finnish	30	97 %
	English	1	3 %
Size of the organisation	Micro	10	32 %
	Small	11	35 %
	Medium	10	32 %
Industry	Industrial	2	6 %
	Construction	1	3 %
	Wholesale and retail trade	3	10 %
	Information and communication	8	26 %
	Finance and insurance operations	1	3 %
	Real estate	1	3 %
	Professional, scientific and technical operations	1	3 %
	Public administration and national defense	2	6 %
	Education	2	6 %
	Other service activities	5	16 %
	Other	5	16 %
Respondent's position in the organisation	Upper management	15	48 %
	Middle management	4	13 %
	Specialist	10	32 %
	Entrepreneur	1	3 %
	Future owner	1	3 %
Organsation's role regarding AI	Provider	12	39 %
	Deployer	21	68 %
	Importer	2	6 %
	Distributor	1	3 %
	Authorized representative	2	6 %
	Connection to the EUDI trust infrastructure	1	3 %
	Design and/or development	2	6 %
	Consulting	1	3 %
	Can't say	6	19 %

Figure 3. Demographics of autumn 2024 questionnaire respondents

In the spring 2025 questionnaire, the respondents were asked to tell if they were a private or a public actor or something else, their size, which sector they operated in, which countries is their organisation located in and in which countries is their organisation operating, providing, or selling products and services. As this study is focused on SMEs, all of the respondents analysed in this study were private actors. Majority of the respondents (58%) represented a micro-sized company, 25% were small and 16% were medium-sized.

49% of the respondents reported that their company operated in multiple sectors. Out of all the respondents, the majority (48%) reported that their company operated in telecommunication, computer programming, consulting, computing infrastructure and other information service activities. Another sector that a large part of the respondents (33%) reported to be operating in was

research and development, 22% reported to be operating in professional, scientific and technical activities, 12% in manufacturing and 12% in education and learning services. Some companies also reported to be operating in several other sectors such as agriculture, forestry and fishing, mining and quarrying, electricity, gas, steam and air conditioning supply, water supply – sewerage, waste management and remediation activities, construction, transportation and storage, publishing, broadcasting and content production and distribution activities, financial and insurance activities, administrative and support service activities, human health and social work activities, arts, sports and recreation, activities of households as employers and undifferentiated goods- and service-producing activities of households for own use, activities of extraterritorial organisations and bodies, human resources, hiring, temping services, military and defence, public administration, traffic, marketing and advertising and medical devices.

Demographics			
		Number	Percentage
Size of the organisation	Micro	39	58 %
	Small	17	25 %
	Medium	11	16 %
Sector	Horizontal (across different industries)	12	18 %
	Agriculture, forestry and fishing	4	6 %
	Mining and quarrying	1	1 %
	Manufacturing	8	12 %
	Electricity, gas, steam and air conditioning supply	7	10 %
	Water supply – sewerage, waste management and remediation activities	1	1 %
	Construction	5	7 %
	Transportation and storage	2	3 %
	Publishing, broadcasting and content production and distribution activities	2	3 %
	Telecommunication, computer programming, consulting, computing infrastructure and other information service activities	32	48 %
	Financial and insurance activities	3	4 %
	Professional, scientific and technical activities	15	22 %
	Administrative and support service activities	1	1 %
	Education and learning services	8	12 %
	Human health and social work activities	6	9 %
	Arts, sports and recreation	2	3 %
	Activities of households as employers and undifferentiated goods- and service-producing activities of households for own use	1	1 %
	Activities of extraterritorial organisations and bodies	1	1 %
	Research & Development	22	33 %
	Human resources, hiring, temping services	1	1 %
	Military and Defence	2	3 %
	Public administration	1	1 %
	Traffic	1	1 %
	Marketing and advertising	1	1 %

Figure 4. Demographics of spring 2025 questionnaire respondents

Regarding the countries and area that the organisations are located and operate in, the respondents could choose a country or countries that are in the European Union, and they could also openly answer if the correct country was not on the list. Most companies (91%), meaning their headquarters and branches, were located in one country. Out of all the respondents, 18% reported their company being in Finland, 18% in Italy and 10% in Germany. Other companies were located around the EU and Europe, and three companies were located outside of Europe, two in the United States and one in Mexico. The following figure presents the locations of respondents' organisations.

Location of the organisation	Austria	4	6 %
	Belgium	5	7 %
	Bulgaria	1	1 %
	Czech Republic	1	1 %
	Estonia	1	1 %
	Finland	12	18 %
	France	3	4 %
	Germany	7	10 %
	Greece	4	6 %
	Hungary	1	1 %
	Ireland	1	1 %
	Italy	12	18 %
	Luxembourg	1	1 %
	Netherlands	2	3 %
	Poland	1	1 %
	Portugal	2	3 %
	Romania	4	6 %
	Slovenia	1	1 %
	Spain	4	6 %
	Sweden	2	3 %
	Mexico	1	1 %
	United States	2	3 %
	Bosnia and Herzegovina	1	1 %
	Norway	2	3 %
	Turkey	1	1 %
	United Kingdom	1	1 %

Figure 5. Location of the spring 2025 questionnaire respondents' organisations

76% of the companies operated in multiple countries, 46% had selected the answer "*All 27 EU member states*" and the rest that operated in multiple countries had selected the specific countries they operated in. 18% of respondents selected that their organisation operates in Finland, 13% in Germany, 12% in France and 10% in Belgium. Almost all of the companies that operated in only one country were also located in the same country, this was a total of 15 companies and out of them seven were Finnish. Only one company was located in a different country that they operated in. Five companies reported that they operated outside of Europe as well, in the United States, Latin

America and Asia. The following figure presents the location of operations of the respondents' organisations.

Location of operations	All 27 EU member states	31	46 %
	Austria	6	9 %
	Belgium	7	10 %
	Bulgaria	2	3 %
	Croatia	1	1 %
	Republic of Cyprus	3	4 %
	Czech Republic	1	1 %
	Denmark	2	3 %
	Estonia	2	3 %
	Finland	12	18 %
	France	8	12 %
	Germany	9	13 %
	Greece	4	6 %
	Hungary	3	4 %
	Ireland	4	6 %
	Italy	5	7 %
	Latvia	1	1 %
	Lithuania	1	1 %
	Luxembourg	3	4 %
	Malta	1	1 %
	Netherlands	5	7 %
	Poland	2	3 %
	Portugal	4	6 %
	Romania	4	6 %
	Slovakia	1	1 %
	Slovenia	3	4 %
	Spain	4	6 %
	Sweden	3	4 %
	United States	2	3 %
	Bosnia and Herzegovina	1	1 %
	United Kingdom	2	3 %
	Serbia	1	1 %

Figure 6. Location of operations of spring 2025 questionnaire respondents' organisations

7.2 General use of AI

The following part of the 2024 questionnaire consisted of clarifying questions about AI and the use of AI in these companies. These questions regarded topics such as the level of AI knowledge and skills among the personnel, knowledge about the different regulations regarding AI and its use, the part of AI in the companies' strategy, important stakeholders in AI projects.

The respondents were asked if they recognise being a provider or a deployer of a high-risk AI system. Most (52%) of respondents did not recognise acting as such and only 16% said yes. The rest of the respondents were unsure, 23% said possibly and 10% said they did not know. It has to be

taken into account that the respondents may not be aware of what is classified as a high-risk AI system as it was not stated in the questionnaire and the respondents weren't asked if they knew what it was.

Regarding the level of AI knowledge and skills among the personnel who take part in the development and use of AI in the company was measured in seven categories. These categories were AI literacy, technical skills, ethical skills, business skills, project management, information management and information analysis and legal and regulatory expertise. The respondents were asked to rate each of the categories on a six-point Likert scale where 1=excellent expertise, 2=good expertise, 3=moderate expertise, 4=minimal expertise, 5=no expertise and 6=I can't say. Most (32%) of respondent reported the AI literacy of their personnel to be good, technical skills were mostly (35%) reported to be moderate and ethical skills were most often (42%) reported to be moderate as well. Business skills of the personnel were most often (48%) reported to be good, most respondents (32%) reported project management to good as well and data management and data analysis was reported to be good by most respondents (32%). Most respondents (32%) reported the legal and regulatory expertise of their personnel was moderate. The median and mode of each category was also calculated and they are presented in figure 8. Interestingly none of the respondents said that their personnel's legal and regulatory expertise was excellent while the other categories were reported to be excellent by at least one respondent. For all categories except one there were 30 respondents, information management and information analysis had 29 respondents.

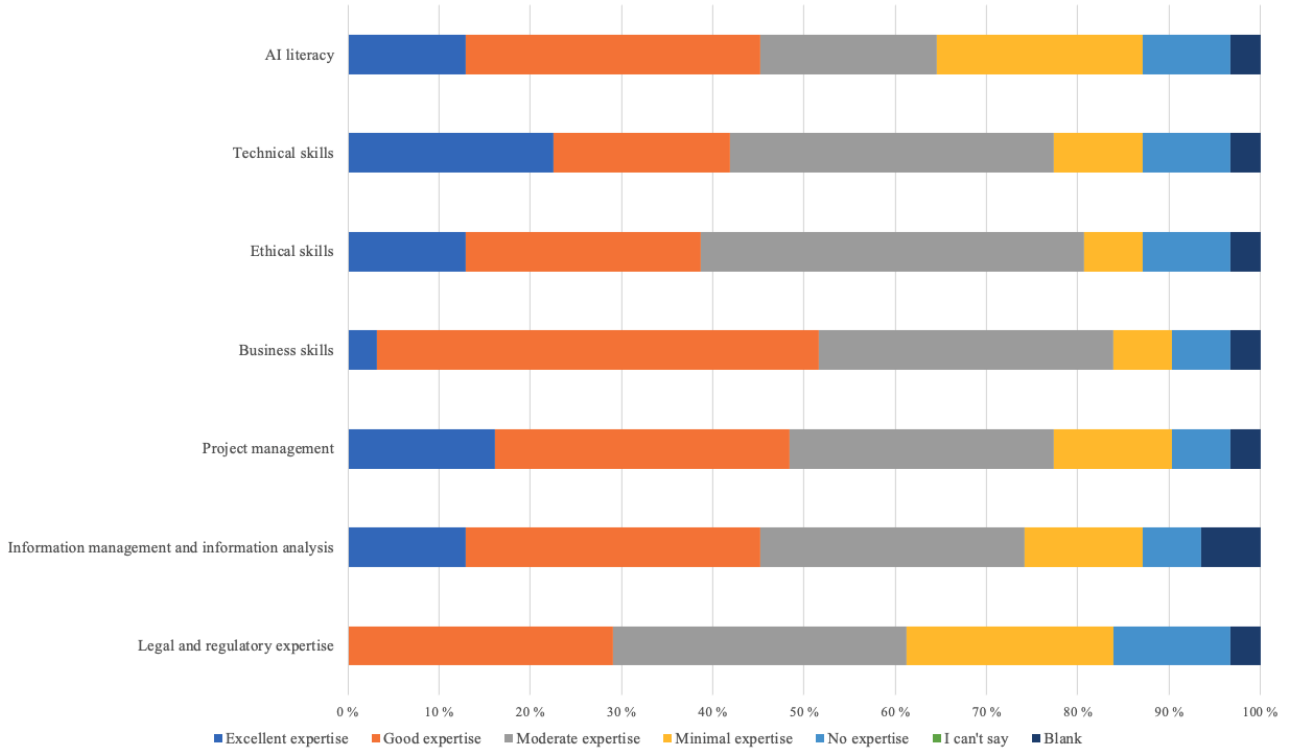

Figure 7. Distribution of responses to the question regarding the level of AI knowledge and skills among personnel

	AI literacy	Technical skills	Ethical skills	Business skills	Project management	Data management and data analysis	Legal and regulatory expertise
Median	3	3	3	2	2,5	3	3
Mode	2	3	3	2	2	2	3

Figure 8. Median and mode of responses to the question regarding the level of AI knowledge and skills among personnel

Regarding the companies' strategy the respondents were asked how AI had been incorporated in it. The answer options were clarified, rules made, planned, tried, deployed, education plan made, other and not incorporated in any way. Most respondents (48%) answered that their company had at least planned some kind of AI to be part of the company's strategy or future plans. 13 respondents reported that they had done multiple of the given options. Only 16% reported that they hadn't incorporated AI in any way into their strategy. Three respondents reported that they had clarified, made rules, planned, tried, deployed and made an education plan regarding the role of AI in their strategy or future plans. When asked about the central stakeholders in the companies' AI projects only 18 respondents answered and 13 did not. This was an open question and thus the respondents had the freedom to answer anything. 23% of respondents said that customers and clients were a central stakeholder regarding their companies' AI projects. 10% also said personnel.

The following part of the autumn 2024 survey aimed to map out the use of AI in the companies more specifically. First, they were asked if their organisation had deployed or developed AI solutions. Majority (71%) of respondents reported that they had done so and the rest (29%) reported that they had not. The most common type of AI solution that the companies used or offered were general-purpose AI solutions such as ChatGPT, 74% of respondents reported to be using or offering such a solution. 42% of respondents also said that they offer general-purpose AI solutions where their organisations' own data was used and 39% of respondents reported that they utilize AI solutions that they had independently developed for their own use. Only in two of the companies there was no AI solution being used or offered.

Regarding the training and development of AI solutions, 39% of respondents reported that they used 1–100 GB of data in training of AI and 35% of respondents answered that they used the amount of conventional server hardware for computing capacity, however, most respondents did not know either the amount of data for training or how big of a computing capacity was needed on average in their organisation. In regard to the time of developing AI solutions, most respondents (29%) reported it to be less than one month, rest of the responses varied quite evenly between 1–3 months (16%), 4–6 months (13%), 7–12 months (10%) and over 12 months (19%), 13% did not answer. New data for training an AI solution was brought in 2–4 times a year by 26% of the companies, however most respondents (42%) did not know how often new data was brought in or did not answer. The life cycle of current AI solutions was not assessed in majority (45%) of the companies. The majority of those who had assessed the life cycle of current AI solutions reported it to be 1–3 years, which was 19% of all respondents.

7.3 AI Regulation

The following part of the autumn 2024 questionnaire aimed to map out the knowledge of regulation surrounding AI. The respondents were asked their knowledge about the EU AI Act, General Data Protection Regulation (GDPR), their own industry's regulation and other regulation such as cyber security and data. The respondents answered using a six-point Likert scale where 1=excellent knowledge, 2=good knowledge, 3=moderate knowledge, 4=minimal knowledge, 5=no knowledge and 6=I can't say. Regarding the AI Act, most respondents (39%) reported their knowledge to be minimal and only 3% of the respondents reported their knowledge to be excellent. Regarding GDPR and the industry specific regulations there were more respondents who reported their knowledge to be excellent, 19% regarding GDPR and 26% regarding the industry specific regulations. The median and mode are presented in the following figure.

	Knowledge of the AIA	Knowledge of the GDPR	Knowledge of own industry's regulation	Knowledge of other regulation (e.g. cyber security, data, sustainability)
Median	4	2	2	3
Mode	4	2	2	3

Figure 9. Median and mode of responses to the question regarding respondents' knowledge on different AI regulation

The respondents were asked rate their organisation's readiness to meet regulatory requirements regarding AI systems on a six-point Likert scale. 1=excellent readiness, 2=good readiness, 3=moderate readiness, 4=minimal readiness, 5=no readiness and 6=I can't say. 26% of respondents reported to have moderate readiness regarding the regulation which makes 3 the mode value of these results. Only 13% said they had no readiness. The calculated median value of 3 gives the same results as the mode.

The respondents were also asked if their organisation used the AI Governance model, AI solutions lifecycle process, compliance assessment process or some equivalent. The majority (61%) reported that they had no such process in place and only 13% said that they had. 26% reported that they are planning to incorporate such a process.

Next, they were asked about the most significant concerns regarding the regulation of AI. The given concerns were information security, risk and impact assessment, transparency of supply chains, increased bureaucracy, data quality and increased costs. They could also give their own answers if they had any. They were asked to rate these concerns on a six-point Likert scale where 1=strongly agree, 2=somewhat agree, 3=neither agree or disagree, 4=somewhat disagree, 5=strongly disagree and 6=I can't say. In all categories except increased bureaucracy the majority of respondents had reported that they somewhat agree it to be a concern. For increased bureaucracy the majority (35%) reported that they strongly agree it to be a concern. Very few, one or two, respondents reported that they strongly disagree any of the given categories to be a concern. The median and mode values were calculated and they are presented in the following figure. The results of this question show that SMEs do have a lot of concerns regarding AI regulation.

	Information security	Risk and impact assessment	Transparency of supply chains	Increased bureaucracy	Data quality	Increased costs
Median	2	2	2	2	2	2
Mode	2	2	2	1	2	2

Figure 10. Median and mode of responses to the question regarding respondents' most significant concerns regarding regulation of AI

In the questionnaire of spring 2025, there was also a question regarding AI regulation. The respondents were presented with the following regulations: the EU AI Act, the general data protection regulation (GDPR), the data act, the digital services act (DSA), the EU Charter of Fundamental Rights, the Cyber Resilience Act, the Directive on copyright in the Digital Single Market, product or industry specific regulations and they were asked to choose which regulations they viewed as most challenging. This question was answered by 59 respondents. Over a half of the respondents (60%) mentioned more than one regulation as challenging. 63% of respondents also said that they see the EU AI Act as challenging. GDPR was viewed as challenging by 33%, product or industry specific regulations were viewed as challenging by 27%, the Cyber Resilience Act by 24% and the Data Act by 18%. 16% reported that they did not know or could not say. Other presented regulations were also seen as challenging by a few companies.

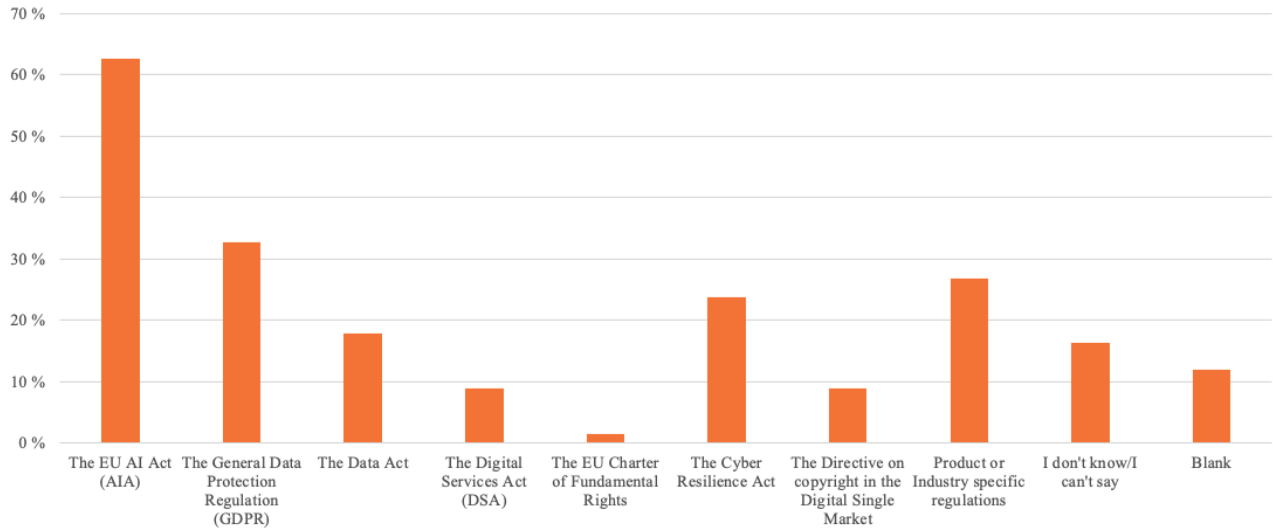

Figure 11. Which regulations do the respondents view the most challenging

The respondents were also able to openly mention any regulations they viewed as challenging and some industry or product specific regulations mentioned were health and medical industry regulations, machinery, finance, banking and trading regulations as well as media and communication related regulations. Additionally, cyber security regulations such as the NIS2 were

mentioned. One respondent also mentioned that they found ultraperipheral regions such as the Canary Islands being a difficult location for AI innovation as the current regulations do not sufficiently take into account the unique economic, environmental and logistical challenges that industries in these locations face. They wished that regulations would be modified in such a way that industries in these locations would not be hindered by them.

7.4 AI development and deployment

First, the results of the autumn 2024 questionnaire will be presented regarding AI development and deployment. A vast majority of respondents (87%) reported that their company is planning to develop or deploy AI solutions and only 13% said no. Regarding the most important objectives in the development and deployment of AI solutions, the respondents were asked to rate how important they viewed the following objectives: improvement of internal operational productivity, development of new or significantly improved products or services and development of entirely new business practices. Respondents were asked to rate these objectives on a six-point Likert scale, where 1=Strongly agree, 2=Somewhat agree, 3=Neither agree or disagree, 4=Somewhat disagree, 5=Strongly disagree and 6=I can't say. This question collected 27 responses; those 4 respondents whose organisation was not planning to develop or deploy AI left this question blank.

For all of the given objectives, the majority of respondents strongly agreed them to be important, 52% for improvement of internal operational productivity, 52% for development of new or significantly improved products or services and 35% for development of entirely new business. The second most respondents reported that they somewhat agreed these objectives to be important, 26%, 23% and 23% respectively. Interestingly 13% said that they neither agreed nor disagreed development of entirely new business to be an important objective and 13% somewhat disagreed it to be important which was more than for the two other objectives. The median and mode of responses was also calculated and are presented in the following figure. From these results it can be seen that most participating companies view the improvement of already existing processes and operations as more important than developing entirely new business practices. However, from the median and the mode it can be seen that the development of entirely new business practices is still viewed as an important goal.

	Improvement of internal operational productivity	Development of new or significantly improved products or services	Development of entirely new business practices
Median	1	1	2
Mode	1	1	1

Figure 12. Median and mode of responses to the question regarding how important the respondents viewed objectives in the development and deployment of AI solutions

Additionally, respondents were asked more specifically about their future plans regarding AI development and deployment. During the next two years, most respondents (45%) said their organisation's number of planned AI solutions was 2–5 solutions and 23% said they had planned 1 AI solution. 4 companies reported that they had planned over 10 AI solutions in the next two years, these were small or medium sized companies. No micro-sized companies reported to have planned more than five AI solutions. This question collected responses from 27 respondents.

When asked about the estimated amount of data to be used in training the planned AI solutions and the estimated computing capacity needed in the development of planned AI solutions, most respondents could not yet say, 42% and 29% respectively reported that they did not know. In terms of the estimated technical development time of the future AI solutions, most respondents (55%) reported it to be 1–6 months, 23% said 1–3 months and 32% said 4–6 months. In regard to how new training data is supposed to be brought in the future AI solutions, most respondents (26%) said 2–4 times a year, however, a noticeable number of respondents (23%) said they could not yet tell.

The next part consists of presenting the results of the spring 2025 questionnaire. Regarding AI development and deployment, the respondents were asked what their organisations stage was in AI development/deployment/integration, what factors refrain their organisation from developing, providing or deploying AI technologies or intending to develop, provide or deploy AI technologies, the number of developed, provided or deployed AI technologies and what kind of AI technologies were their company developing, providing or deploying or intending to develop, provide or deploy. Additionally, they were asked if they knew the risk level of their AI system or their general-purpose AI model as per the AI Act, the amount of time it would take to develop their AI technology and was their organisation aiming to become an AI provider, an AI deployer, or both.

Regarding the organisations stage in AI development, deployment or integration, the respondents were able to choose already developed or deployed AI technologies, currently developing AI technologies (not yet released in the market), intends to or thinks of developing and deploying AI

technologies or does not develop or deploy nor aims to develop or deploy AI technologies. Majority of respondents (46%) reported that their company has already developed or deployed AI technologies, 36% are currently developing AI technologies that are not yet released in the market, 19% intends to develop or deploy AI technologies and 12% reported that their company does not develop or deploy AI technologies and is not aiming to do so either. 6 respondents selected more than one option.

The eight respondents who reported that their company does not develop or deploy AI technologies nor aims to do so were able to tell their reasons for this. The most common reason was lack of resources to comply with regulatory requirements, four respondents reported this. Three respondents also reported lack of skilled labour being a barrier, two reported lack of organisation's technical knowledge as a barrier and two of the companies simply did not want or need to develop or deploy AI technologies.

31 out of the 67 respondents reported how many AI technologies their company had developed, provided or deployed and the majority of these respondents, 27 companies, had developed, provided or deployed 1–10 AI technologies and four companies had developed over ten AI technologies. Interestingly, two of the companies who had developed, provided or deployed the most AI technologies, 100 and 85 technologies, were both micro-sized companies.

Next, the respondents were asked if their company was developing, providing or deploying or intending to develop, provide or deploy either general-purpose AI models or AI systems with a designated purpose. Clear majority of 70% reported that their company was developing, providing or deploying or intending to develop, provide or deploy an AI system with a designated purpose. 18% reported general-purpose AI model. This question was answered by 59 respondents.

The following questions mapped out the risk levels of the respondents' companies' AI systems and general-purpose AI models. Regarding their AI systems, one third (33%) of respondents either did not know the risk level or left the question blank. 3% reported that they did not know and 30% left this question blank. 27% said their AI systems were minimal risk AI systems, 30% said limited risk, 9% high-risk and one respondent said that their company's AI system was categorised as prohibited practices. The respondents were also asked to tell if they knew their companies' general-purpose AI (GPAI) model's risk level. Only 11 respondents answered to this question. 4% of respondents reported that did not know, 7% said their GPAI was without a systemic risk, 3% said their GPAI was with a systemic risk and one respondent said their GPAI model was classified as prohibited

practices. However, it cannot be verified that the respondents are aware of what the risk categories presented in the AI Act are, so these results may not be taken as a fact.

Regarding the development time of their AI technologies, the respondents were asked how long it does, did or would take them to develop their AI technologies. This question was answered by 59 respondents. 27% of respondents reported their company's development time being 6–12 months, 22% said 12–24 months, 12% 3–6 months, 10% 1–3 months and 13% over 2 years. Next, the respondents were asked if their organisation is or is aiming to become an AI provider, an AI deployer or both. Again, 59 respondents answered to this question. 40% of the companies were or aimed to be both a provider and a deployer, 28% were or aimed to be AI providers and 16% AI deployers.

7.5 Challenges of AI development and deployment

The respondents of the autumn 2024 questionnaire were asked to rate which challenges they had faced during the development and deployment of AI solutions. The given challenges were lack of quality data, capacity issues, challenges related to regulation, business benefit and lack of knowledge and skills. The respondents were also able to give their own answers. They were able to rate each challenge on a six-point Liker scale where 1=strongly agree, 2=somewhat agree, 3=neither agree or disagree, 4=somewhat disagree 5=strongly disagree and 6=I can't say. This question was responded by all 31 of respondents.

Regarding lack of quality data, most respondents (39%) answered somewhat agree and 19% said strongly agree. Capacity issues were seen as less of a challenge, the majority (26%) answered somewhat disagree, however, 13% responded that they strongly agree it to be a challenge and 16% said they somewhat agree. Regulatory challenges were seen as somewhat challenging, 23% reported that they strongly agreed and 23% somewhat agreed, however the majority (29%) said that they neither agreed nor disagreed. This could be indicative of lack of knowledge about AI regulation among respondents and this also correlates to the level of knowledge about the AI Act that these companies have, 39% said they had minimal knowledge.

Business benefit was somewhat agreed to be a challenge by the majority (26%) of respondents, 23% of respondents neither agreed nor disagreed and 19% somewhat disagreed. Lack of knowledge and skills was somewhat agreed to be a challenge by 35% of the respondents and 13% strongly agreed it to be a challenge. Only 6% of the respondents could not say if they thought the lack of knowledge and skills was a challenge while for the other presented challenges the share who answered "I can't

say" was higher. Two of the respondents had also mentioned costs to be a challenge and other two had brought up customer needs as challenging. Their concerns were "customer suspicion" and "meeting needs". Lack of quality data was the only issue where majority (58%) either strongly or somewhat agreed it to be a challenge, for lack of knowledge and skills this share was almost half, 48% of respondents. Very few of the respondents, either none, two or three, selected strongly disagree to any of the presented challenges. Lack of quality data faced most from these presented challenges. The median, mode and distribution of responses are presented in the following two figures.

	Lack of quality data	Capacity issues	Regulatory challenges	Business benefit	Lack of knowledge and skills
Median	2	4	3	3	3
Mode	2	4	3	2	2

Figure 13. Median and mode of responses to the question regarding which challenges the respondents had faced during the development and deployment of AI solutions

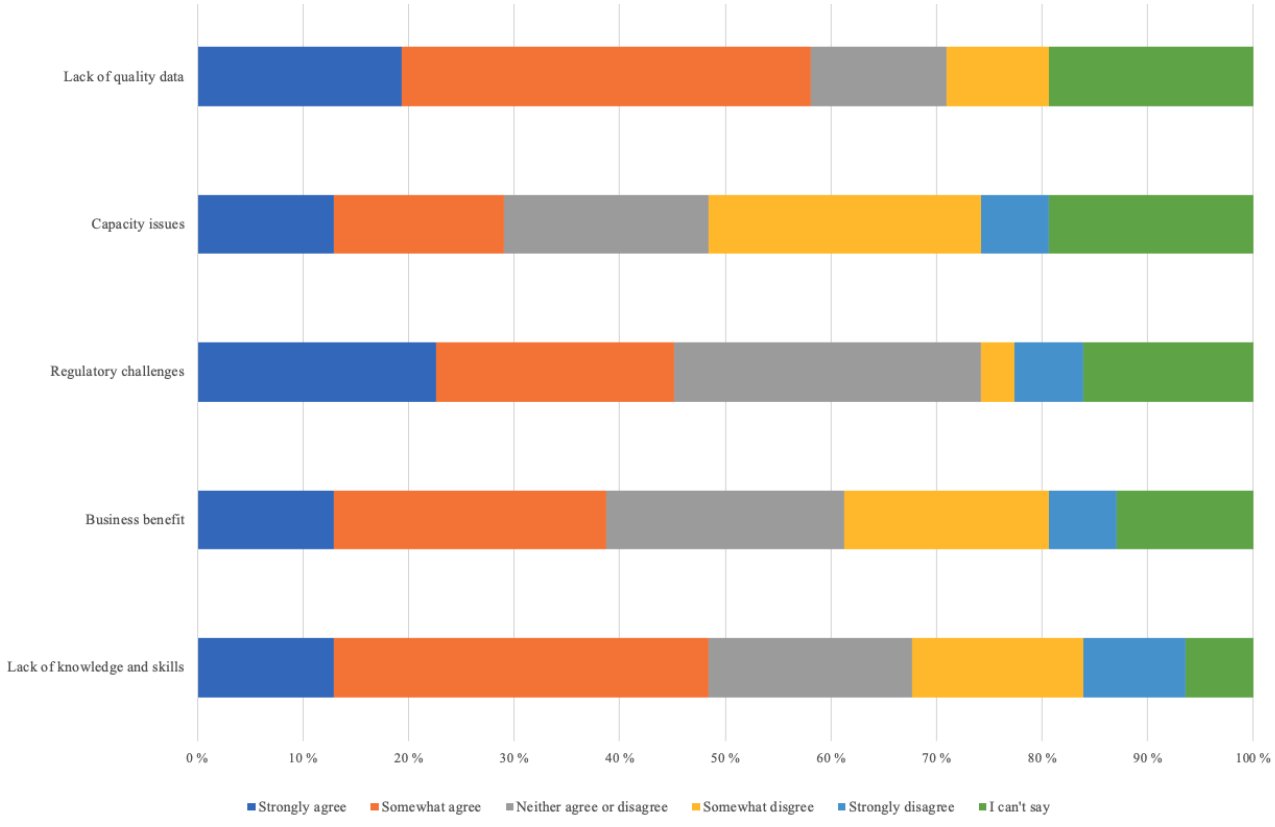

Figure 14. Distribution of responses to the question regarding which challenges the respondents had faced during the development and deployment of AI solutions

The spring 2025 questionnaire also had a question regarding challenges that companies were facing or anticipated to face as an AI provider or a deployer. The respondents were presented with the following challenges: lack of financial resources for technical developments, lack of financial

resources for operations, lack of understanding of, or (financial) resources for, legal compliance, lack of competitiveness of the AI solution compared to existing ones, lack of skilled labour with technical knowledge to develop/deploy a competitive solution, lack of skilled labour to undertake regulatory compliance and obligations, lack of skilled labour with interdisciplinary knowledge to understand and manage AI risks, lack of guidance from national authorities (e.g. who to contact for legal clarifications, ...), absence of a safe testing facility where AI solutions can be tested without concerns regarding legal implications, lack of risk management systems and tools, to mitigate risks and monitor them, absence of clear metrics and standardised evaluation frameworks for self-assessing AI solutions and lack of networks to exchange and learn from best practices. They were then asked to rate each challenge on a five-point Likert scale where 1=not challenging, 2=slightly challenging, 3=challenging, 4=significantly challenging and 5=extremely challenging.

This question was answered by 59 respondents. 25% of respondents viewed lack of financial resources for technical developments as challenging and 25% as significantly challenging. 16% rated extremely challenging and 15% slightly challenging, only 6% said not challenging. Similarly, lack of financial resources for operations was rated as challenging by 25% of the respondents, significantly challenging by 22%, slightly challenging by 16%, extremely challenging by 15% and 9% rated not challenging. 27% of respondents rated lack of understanding of, or (financial) resources for, legal compliance as significantly challenging, 19% rated challenging, 18% slightly challenging, 16% as extremely challenging and 7% as not challenging. Lack of competitiveness of the AI solution compared to existing ones was viewed as challenging by 24% of respondents, slightly challenging by 24%, significantly challenging by 16%, extremely challenging by 10% and not challenging by 13%.

Lack of skilled labour with technical knowledge to develop/deploy a competitive solution was rated as challenging by 22% of respondents, slightly challenging by another 22%, significantly challenging by 16%, extremely challenging by 13% and not challenging by 13%. Lack of skilled labour to undertake regulatory compliance and obligations was a bit more evenly rated. 19% said extremely challenging, 19% significantly challenging, 19% slightly challenging, 18% challenging and 12% not challenging. The majority of respondents (25%) viewed the lack of skilled labour with interdisciplinary knowledge to understand and manage AI risks as slightly challenging, 22% as significantly challenging, 18% as challenging, 15% as extremely challenging and 7% as not challenging.

Lack of guidance from national authorities was rated significantly challenging by 28% of respondents, extremely challenging by 24%, slightly challenging by 16%, challenging by 10% and not challenging by 9%. Absence of a safe testing facility where AI solutions can be tested without concerns regarding legal implications was rated as extremely challenging by 21% of the respondents, challenging by 19%, slightly challenging by 19%, significantly challenging by 15% and not challenging by 13%. 24% of respondents said that lack of risk management systems and tools, to mitigate risks and monitor them was slightly challenging, 22% reported it to be challenging, 16% extremely challenging, 13% significantly challenging and 12% not challenging. Absence of clear metrics and standardised evaluation frameworks for self-assessing AI solutions was rated as challenging by 30% of respondents, extremely challenging by 19%, significantly challenging by 19%, slightly challenging by 12% and not challenging by 7%. Lack of networks to exchange and learn from best practices was viewed as slightly challenging by 24% of respondents, significantly challenging by 22%, challenging by 21%, extremely challenging by 13% and not challenging by 7%. The median, mode and distribution of responses are presented in the following figures.

	Lack of financial resources for technical developments	Lack of financial resources for operations	Lack of understanding of, or (financial) resources for, legal compliance	Lack of competitiveness of the AI solution compared to existing ones	Lack of skilled labor with technical knowledge to develop/deploy a competitive solution	Lack of skilled labour to undertake regulatory compliance and obligations	Lack of skilled labor with interdisciplinary knowledge to understand and manage AI risks	Lack of guidance from national authorities (e.g. who to contact for legal clarifications, ...)	Absence of a safe testing facility where AI solutions can be tested without concerns regarding legal implications	Lack of risk management systems and tools, to mitigate risks and monitor them	Absence of clear metrics and standardised evaluation frameworks for self-assessing AI solutions	Lack of networks to exchange and learn from best practices
Median	3	3	3	3	3	3	3	4	3	3	3	3
Mode	3	3	4	2	2	5	2	4	5	2	3	2

Figure 15. Median and mode of responses to the question regarding challenges that companies were facing or anticipated to face as an AI provider or a deployer

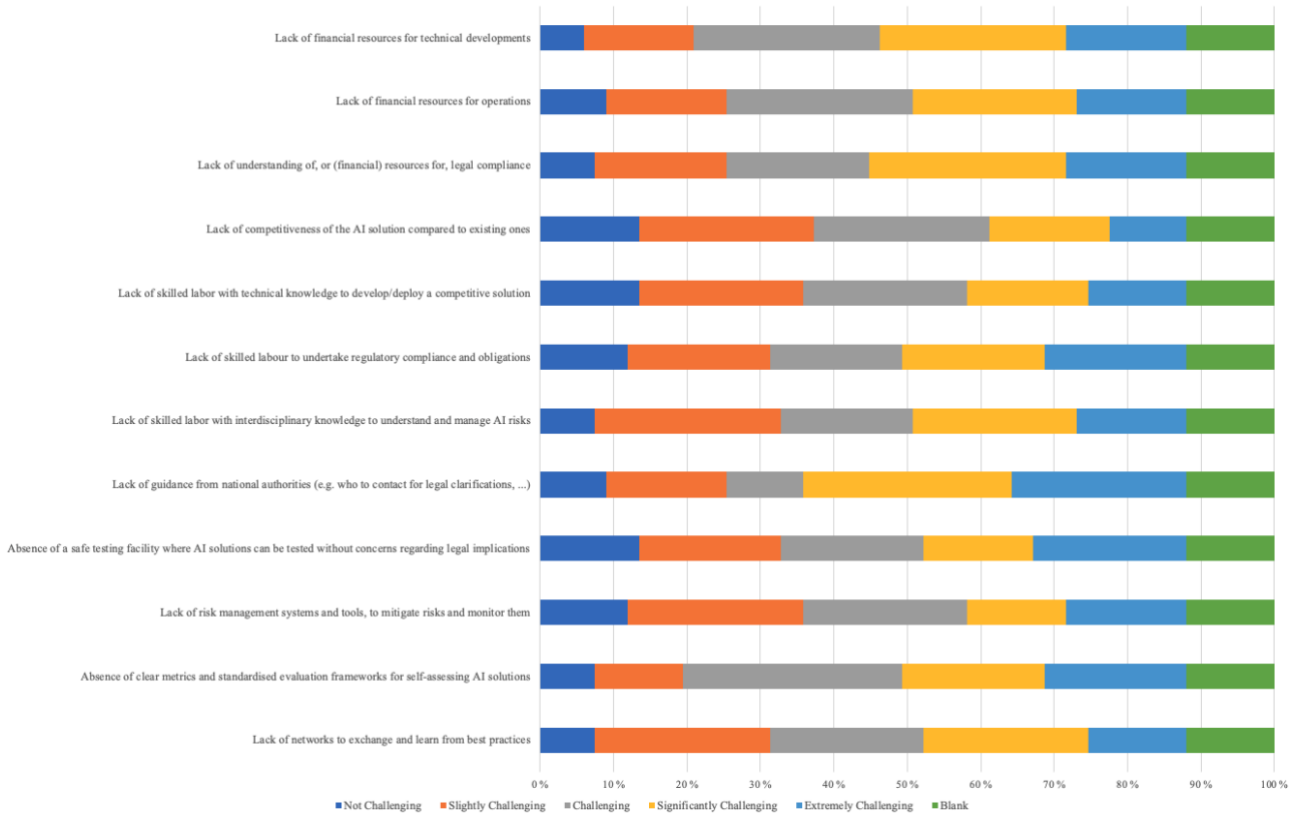

Figure 16. Distribution of responses to the question regarding challenges that companies were facing or anticipated to face as an AI provider or a deployer

The respondents were also able to freely express any other challenges that they are or would be facing as an AI provider or deployer. 26 respondents mentioned some other challenges and one clear common theme that several respondents had mentioned was that they found the risk categories in the AI Act quite difficult to interpret and the borders between them should be clarified. There were also a few answers regarding clients and customers, such as difficulty finding new customers and identifying them along the value chain. Additionally, there were mentions of the lack of flexible regulatory frameworks, costly and time-consuming certificates, and lack of understanding all the different regulations that a product must comply with. The lack of harmonised standards between industries was also mentioned a challenge.

From these results it can be seen that most respondents see these issues as challenging to at least some degree. Lack of guidance from national authorities was seen as most challenging. Absence of a safe testing facility where AI solutions can be tested without concerns regarding legal implications was seen as extremely challenging by quite a few respondents as well. Interestingly, absence of a safe testing facility where AI solutions can be tested without concerns regarding legal implications was also seen as not challenging by more respondents than the other issues, only lack of competitiveness of the AI solution compared to existing ones and lack of skilled labour with

technical knowledge to develop/deploy a competitive solution were seen as not challenging by the same number of respondents.

7.6 The AI regulatory sandbox

In the final part of the autumn 2024 questionnaire, the participants were asked about their opinions on the AI Act regulatory sandbox. First, they were asked how important their organisation viewed the possibility of being able to test and develop AI solutions in a safe and controlled AI regulatory sandbox. The respondents were asked to rate how important they perceived the sandbox participation on a six-point Likert scale, where 1=extremely important, 2=quite important, 3=neutral, 4=quite unimportant, 5=extremely unimportant and 6=I can't say. All 31 respondents responded to this question. The majority (35%) rated the importance to be quite important, 29% said extremely important, 16% said neutral, 13% could not say and only 3% said quite unimportant and 3% said extremely unimportant. The median value of these responses was 2. It is clear that the majority of respondents viewed the opportunity to participate in a regulatory sandbox as important for their organisation.

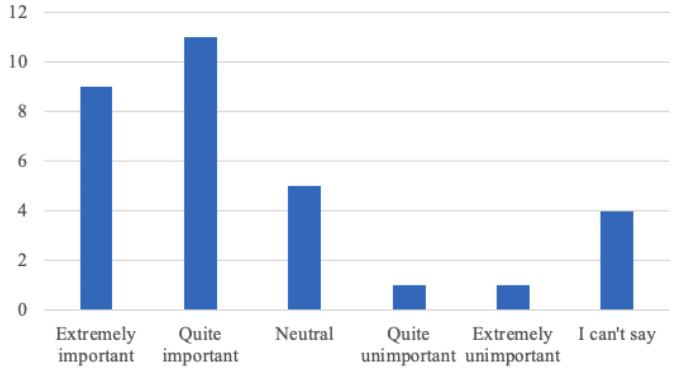

Figure 17. Distribution of responses to the question regarding how important the respondents' organisations viewed the possibility of being able to test and develop their AI solutions in the AI regulatory sandboxes

Next, the respondents were asked if their organisation was planning to conduct a compliance assessment of their AI solution using the AI regulatory sandbox. Answer options were 1=always, 2=in most cases, 3=in around half of the cases, 4=in some cases, 5=never and 6=I can't say. This question was also answered by all 31 respondents. A clear majority (55%) could not yet say if they were going to utilise the sandbox which could be attributed to the fact that the AI regulatory sandbox is a relatively new thing and not yet in effect. However, 13% already said that their organisation was going to use the sandbox in most cases, 13% said in some cases, 10% said always, 6% said in around half of the cases and only one participant (3%) said never.

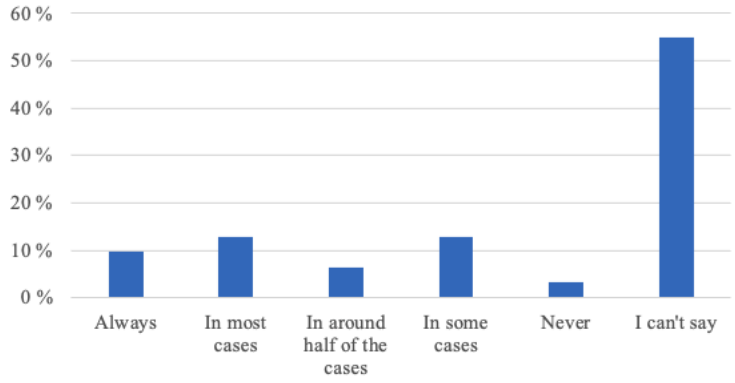

Figure 18. Distribution of responses to the question regarding if the respondents' organisations were planning to conduct a compliance assessment of their AI solution using the AI regulatory sandbox

The respondents were then presented with 13 services that the regulatory sandbox provides and asked to rate how important they viewed each service. The presented services were ready-made development environments and sufficient capacity, ready-made processes and best practices, guidance (risk identification, compliance, guidance on finding standards), simpler bureaucracy, reduced costs, accelerated turnaround time (from application process to market entry), service in Finnish, authorities and other actors in the same place, final report that can be used in compliance assessment, freedom from certain requirements and consequences during the development process, possibility to utilise personal data in AI development, improved legal certainty and immunity from penalties and testing of new solutions. This question also utilised the Likert scale and the answer options were 1=extremely important, 2=quite important, 3=neutral, 4=quite unimportant, 5=extremely unimportant and 6=I can't say. All 31 respondents answered this question.

For ready-made development environments and sufficient capacity, a clear majority of 55% rated it to be extremely important, 19% rated quite important, 13% could not say, 10% were neutral and only 3% viewed it as quite unimportant. Ready-made processes and best practices were rated extremely important by the majority of 42%, 26% were neutral, 19% rated quite important, 10% could not say and 3% rated quite unimportant. Guidance (risk identification, compliance, guidance on finding standards) was also rated to be extremely important by the majority of respondents (52%), 23% viewed it as quite important, 13% rated neutral, 10% could not say and 3% rated quite unimportant. Clear majority of 52% rated simpler bureaucracy to be extremely important, 26% said quite important, 10% rated quite unimportant, 10% could not say and 3% were neutral. Reduced costs were also rated to be extremely important by the majority (45%), 29% viewed them as quite important, 10% as quite unimportant, 10% could not say and 6% were neutral.

Accelerated turnaround time (from application process to market entry) was rated to be quite important by the majority of 32%, almost an equal number of respondents (29%) rated it to be extremely important, 19% were neutral, 16% could not say and 3% rated quite unimportant. The importance of receiving service in Finnish was seen as somewhat less important than the previous services, only 26% rated it to be quite important, 23% as extremely important, 19% as extremely unimportant, 16% were neutral, 10% said quite unimportant and 6% could not say. Authorities and other actors being in the same place was seen as quite important by 39% of respondents, 26% rated it to be extremely important, 13% were neutral, 13% could not say, 6% rated quite unimportant and 3% rated extremely unimportant. Getting a final report to be used in compliance assessment was rated to be quite important by 35% of respondents, 32% rated extremely important, 16% could not say, 10% were neutral and 6% said quite unimportant.

Freedom from certain requirements and consequences during the development process was seen as extremely important by the majority of respondents (39%), 23% rated quite important, 16% were neutral, 13 % could not say and 10 % rated quite unimportant. 35% of respondents viewed the possibility to utilise personal data in AI development as extremely important, 23% were neutral, 19% could not say, 10% rated extremely unimportant, 6% said quite important and 6% said quite unimportant. Improved legal certainty and immunity from penalties was rated to be quite important by 39% of respondents, 32% rated extremely important, 19% could not say, 6% were neutral and 3% rated quite unimportant. Testing of new solutions was seen as extremely important by a clear majority of 55%, 23% viewed it as quite important, 10% rated neutral, 10% could not say and 3% rated quite unimportant.

	Ready-made development environments and sufficient capacity	Ready-made processes and best practices	Guidance (risk identification, compliance, guidance on finding standards),	Simpler bureaucracy	Reduced costs	Accelerated turnaround time (from application process to market entry)	Service in Finnish	Authorities and other actors in the same place	Final report that can be used in compliance assessment	Freedom from certain requirements and consequences during the development process	Possibility to utilise personal data in AI development	Improved legal certainty and immunity from penalties	Testing of new solutions
Median	1	2	1	1	2	2	3	2	2	2	3	2	1
Mode	1	1	1	1	1	2	2	2	2	1	1	2	1

Figure 19. Median and mode of responses regarding how important the respondents viewed services that the regulatory sandbox provides

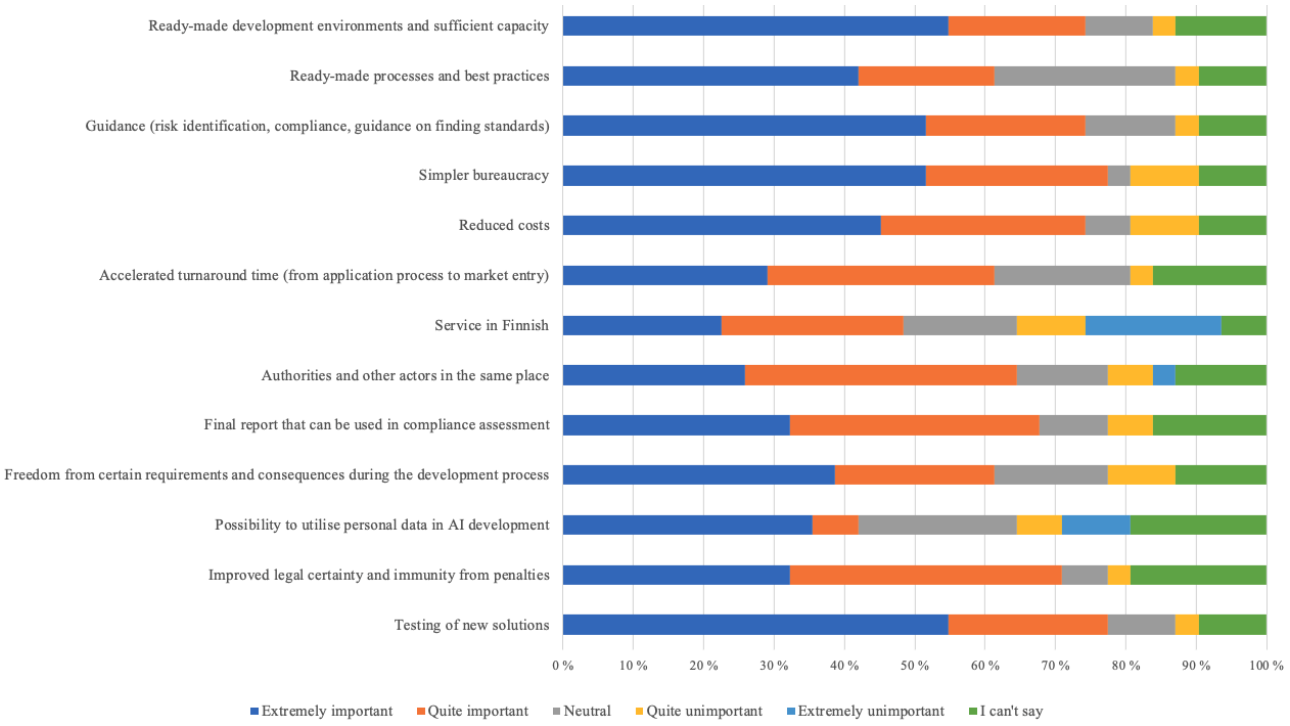

Figure 20. Distribution of responses regarding how important the respondents viewed services that the regulatory sandbox provides

It can be seen from these results that most representatives of SMEs view most of these services as extremely important or quite important. Only the possibility to utilise personal data in AI development and ready-made processes and best practices were rated neutral more often than quite important, however, they were still rated extremely important by the majority. Most important services for these respondents were clearly ready-made development environments and sufficient capacity, ready-made processes and best practices, guidance (risk identification, compliance, guidance on finding standards), simpler bureaucracy, reduced costs and testing of new solutions. It can be seen from this that the respondents are clearly more interested in the regulatory sandbox as a place to develop and test new AI innovations and the regulatory learning seems to be a secondary service. Interestingly, only three services, service in Finnish, possibility to utilise personal data in AI development, authorities and other actors in the same place, were seen as extremely unimportant by some of the respondents. Receiving service in Finnish was clearly the least important of the presented services.

The respondents were asked if they thought that industry specific AI regulatory sandboxes were needed. 52% of respondents could not say, 42% said yes and 6% left it blank. Those who left it blank had reported that their organisation had not planned to develop or deploy AI solutions. None of the respondents said no.

Regarding the cost of entering a regulatory sandbox, the respondents were asked if they would participate in a sandbox if they had to pay for it. The EU AI Act states that SMEs can enter the regulatory sandbox free of charge (Small Businesses' guide to the AI Act, 2025). 45% reported that they could not say if they would participate in a such case, quite a large portion of 32% said no and only 16% said yes. 2 respondents left this question blank. Next the respondents were asked if they thought that the regulatory sandbox should allow testing of AI solutions regarding other national and EU regulations. Majority of 45% could not say, 35% reported yes if it was free and 19% said yes and they were ready to pay for it. Regarding the questions about having to pay to enter regulatory sandboxes or to use their added services only some of the small and medium-sized companies reported that they were willing to pay. No micro-sized companies reported being willing to pay for these services.

Next, the respondents could openly tell what national and EU regulations the AI regulatory sandbox should support testing for. Six respondents had answered to this question and five of them had mentioned the GDPR, one had mentioned general EU compliance, and one mentioned the EU Digital Services Act (DSA) and the EU Cybersecurity directive NIS2.

The respondents were then asked if their organisation would be willing to participate in a regulatory sandbox managed by another EU member state if it was open to Finnish actors. 48% reported that they would choose on a case-by-case basis, 35% could not say and 16% said that they would do it if Finland did not have its own regulatory sandbox.

Finally, the respondents were able to openly tell any development proposals for improving the regulatory sandboxes and if they wished to receive regulatory advice from a specific authority. Ten respondents had answered to the question regarding the development proposals, and they had mentioned the following themes. The infrastructure of Finnish regulatory sandboxes should be unified for several reasons: cost effectiveness, unified standards to ensure that all actors obey the same ethical and technical standards, supervision of Traficom (the Finnish Transport and Communications Agency), fair competition, national competitiveness and innovation and safety. These would promote trustworthiness, fair competition and accelerate innovation. The regulatory sandbox should have clear objectives such as accelerated time-to-market and certificates. The testing should be as realistic as possible, and it should involve ethical and societal effects. The sandbox should promote collaboration between stakeholders through, for example, workshops and open communication. The sandbox should promote commercialisation of innovations and simplify regulatory processes by creating a sustainable and scalable platform. Additionally, the sandbox

should be able to support different business regulatory aspects, it should be open-source code so that different stakeholders could contribute to the implementation work and SMEs should receive clear instructions.

It was also mentioned by a respondent that in their opinion the AI Act is too complicated in its current from and it should be simplified, otherwise it is detrimental to European competitiveness. Additionally, they thought that there should be a regulatory sandbox in every industry, they should be free of charge and there should be a warranty/insurance system to protect the company after they enter the market. Another also mentioned that the sandbox should not become too bureaucratic.

Seven respondents answered to the question about specific authorities and several Finnish and international actors were mentioned: Business Finland, Traficom, the Ministy of Economic Affairs and Employment of Finland (TEM), data protection authority, Finnish Competition and Consumer Authority (KKV) and international regulatory authority. Some had also mentioned that they wished to receive clear guidance on what could become regulatory issues, but also to have sufficient freedom to innovate, understanding of when to use the regulatory sandbox.

From these responses it can be seen that the SMEs want clear and understandable instructions and guidance regarding the regulatory sandbox process. They also want the regulatory sandbox to bring them value, such as better innovation and accelerated time-to-market. It should also be clarified when the sandbox process is necessary, and this requires clear information on the different risk categories of AI systems mentioned in the AI Act.

Next, the results of the spring 2025 questionnaire are presented regarding the questions that concern the AI regulatory sandbox. In this questionnaire, the respondents were asked if they knew what an AI regulatory sandbox was, what does it mean to them, how they would evaluate certain benefits of the regulatory sandbox, which mechanisms of the sandbox would be most helpful and which areas and how much they would expect to save time when participating in a sandbox. Additionally, they were asked if they would be willing to cover any costs of participating in the sandbox.

49% of respondents reported that they knew what an AI regulatory sandbox was, 39% reported that they did not know and 12% of respondents, those who reported that they were not developing or deploying nor aiming to develop or deploy AI technologies, left this question blank. The same 12% also left all of the following questions blank.

The respondents were then presented with the following options for what an AI regulatory sandbox meant to them: a controlled environment (digital or physical) to safely develop AI technologies, a

controlled environment (digital or physical) to train AI technologies, a controlled environment (digital or physical) to test AI technologies, a controlled environment (digital or physical) to validate AI technologies, a safe space to develop, test or validate AI systems without legal implications (e.g. fines...), a safe space to legally and ethically develop, train, test, and/or validate AI technologies, a safe space to have close cooperation with AI Act supervisory authorities, an information point on the AI Act and a mechanism to get an AI system approved and CE-marked. The respondents were asked to choose those options that they thought a regulatory sandbox meant.

This question was answered by 33 respondents, those who reported that their organisation was not developing or deploying nor aiming to develop or deploy AI technologies and those who did not know what a regulatory sandbox was left this question blank. The most chosen option was a safe space/controlled environment to develop, test or validate AI systems without legal implications and this was chosen by 19 respondents. A controlled environment (digital or physical) to safely develop AI technologies and a safe space to have close cooperation with AI Act supervisory authorities were chosen by 14 respondents each. A controlled environment (digital or physical) to test AI technologies was chosen by 11 respondents and a controlled environment (digital or physical) to validate AI technologies was selected by 10 respondents. These were clearly the most selected options; however, the rest were also selected by some respondents. A controlled environment (digital or physical) to train AI technologies was selected by 5 respondents, a mechanism to get an AI system approved and CE-marked by 4 and a safe space to legally and ethically develop, train, test, and/or validate AI technologies and an information point on the AI Act were both selected by 3 respondents each. Based on these results, the respondents value the safe and controlled environment where they can develop, test and validate their AI technologies without having to worry about the legal implications that the sandbox provides.

The next question regarded how beneficial the respondents saw different benefits of their organisation’s participation in a regulatory sandbox. The benefits provided in the questionnaire were: reduce the time taken to develop, train, test, and/or validate your AI technologies, reduce your organisation's upskilling/hiring efforts, reduce the cost of compliance, ease the bureaucratic process for compliance, improve legal certainty and compliance confidence, provide your feedback to authorities on the feasibility of regulation, improve your organisational trust, simplify access to real-world testing and enhance your organisation's visibility and networking. The respondents were then asked to rate each benefit on a five-point Likert scale where 1=not beneficial, 2=slightly beneficial, 3=beneficial, 4=very beneficial and 5=with exceptional added value.

59 respondents answered this question. Reduce the time taken to develop, train, test and/or validate your AI technologies was rated to be very beneficial 27% of respondents, beneficial by 24%, with exceptional added value by 15%, slightly beneficial by 13% and not beneficial by 9%. Reduce your organisation's upskilling/hiring efforts was rated as beneficial by 28% of respondents, not beneficial by 21%, slightly beneficial by 15%, with exceptional added value by 13% and very beneficial by 10%. Reduce the cost of compliance was rated as very beneficial by 28% of respondents, beneficial by 22%, with exceptional added value by 22%, slightly beneficial by 10% and not beneficial by 4%. 31% of respondents rated ease the bureaucratic process for compliance as very beneficial, 21% as with exceptional added value, another 21% as beneficial, 9% as not beneficial and 6% as slightly beneficial.

Improve legal certainty and compliance confidence was rated as beneficial by 30% of respondents, with exceptional added value by 28%, very beneficial by 19%, slightly beneficial by 6% and not beneficial by 4%. Provide your feedback to authorities on the feasibility of regulation was seen as very beneficial by 27% of respondents, beneficial by 24%, with exceptional added value by 16%, slightly beneficial by 12% and not beneficial by 9%. 33% of respondents reported that they viewed improving your organisational trust as very beneficial, 22% as beneficial, 13% as with exceptional added value, 12% as slightly beneficial and 7% as not beneficial. Simplify access to real-world testing was rated as very beneficial by 30% of respondents, beneficial by 24%, with exceptional added value by 15%, slightly beneficial by 9% and not beneficial by 9%. Enhance your organisation's visibility and networking was rated as beneficial by 30% of respondents, very beneficial by 25%, with exceptional added value by 15%, slightly beneficial by 13% and not beneficial by 4%. The median and mode values as well as the distribution of responses are presented in the following figures.

	Reduce the time taken to develop, train, test, and/or validate your AI technologies	Reduce your organisation's upskilling/hiring efforts	Reduce the cost of compliance	Ease the bureaucratic process for compliance	Improve legal certainty and compliance confidence	Provide your feedback to authorities on the feasibility of regulation	Improve your organisational trust	Simplify access to real-world testing	Enhance your organisation's visibility and networking
Median	3	3	4	4	4	3	4	4	3
Mode	4	3	4	4	3	4	4	4	3

Figure 21. Median and mode of responses to the question regarding how beneficial the respondents viewed different benefits of their organisation's participation in a regulatory sandbox

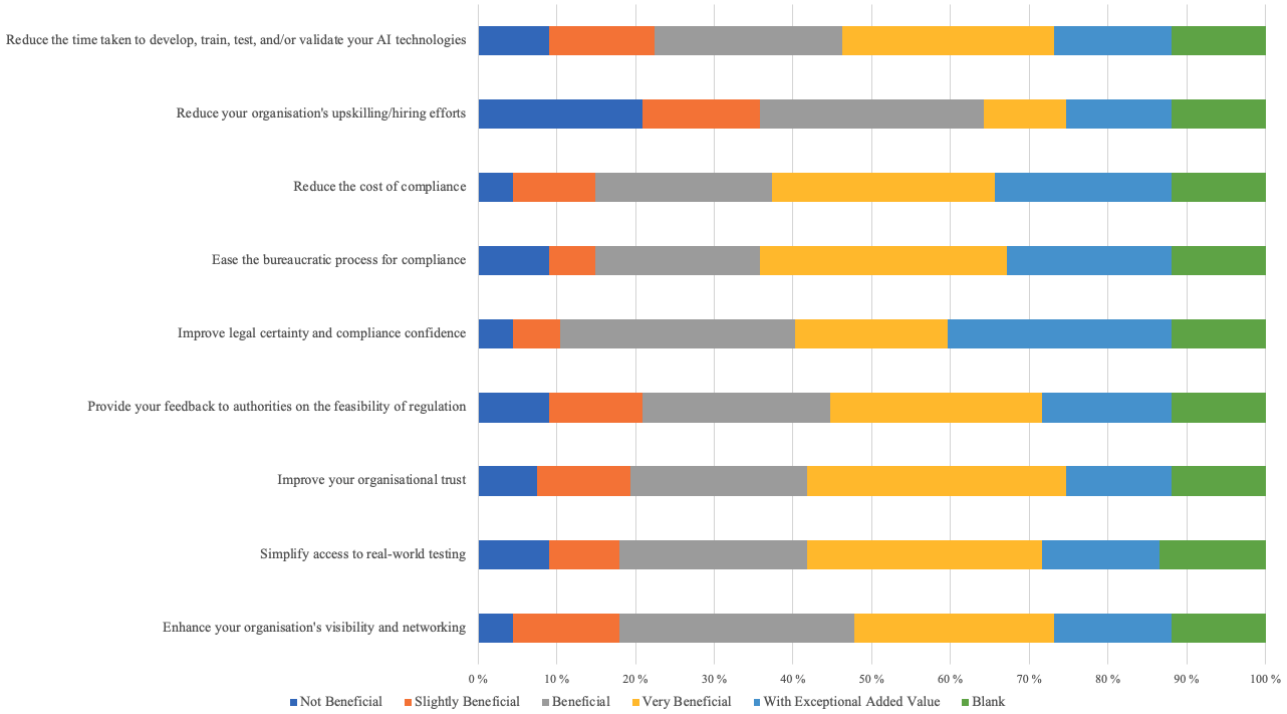

Figure 22. Distribution of responses to the question regarding how beneficial the respondents viewed different benefits of their organisation's participation in a regulatory sandbox

The respondents were also able to openly tell any benefits they thought participating in a regulatory sandbox would offer. 16 respondents had provided their own additional benefits, and some benefits mentioned were removing sales barriers and finding new customers, being an early adopter of new AI technologies and gaining competitive advantage, easy AI adoption, gaining access to different industries and aid in creating new compliant products. Two respondents mentioned the need to fully understand how the regulatory sandbox works and what value it can provide.

From these results it can be seen that the majority of respondents valued these benefits to at least some extent. Improving legal certainty and compliance confidence was rated to be with exceptional added value the most. Two other benefits that these respondents seem to value the most were easing the bureaucratic process for compliance and reducing the cost of compliance. Reducing the organisation's upskilling/hiring efforts was seen as the least beneficial by these respondents

Similarly to the previous question, in the next question the respondents were also presented with various propositions and asked to rate them. These propositions regarded mechanisms that would be most helpful in a sandbox for the participants' organisations. These propositions were: identifying the risk level, including high-risk systems, of my AI technologies, as per the AI Act, general guidance on how to comply with the AI Act, in-depth guidance on how to comply with different requirements of the AI Act (e.g. for high-risk AI Systems; Risk Management system, Fundamental

Rights Impact Assessment...), evaluating my compliance with the AI Act, identification, assessment, management, and (guidance on) ongoing monitoring of AI risks, in compliance with the AI Act, staying in contact with authorities, receiving clear guidance from authorities on how to comply with the GDPR and related data requirements and navigating the intersection between different laws. The respondents were asked to rate each of these propositions on a five-point Likert scale, where 1=not helpful, 2=slightly helpful, 3=helpful, 4=very helpful and 5=extremely helpful.

59 respondents answered this question. Identifying the risk level, including high-risk systems, of my AI technologies, as per the AI Act was rated helpful by 28% of respondents, extremely helpful by 21%, very helpful by 19%, slightly helpful by 13% and not helpful by 6%. General guidance on how to comply with the AI Act was rated very helpful by 30% of respondents, helpful by 25%, extremely helpful by 22%, slightly helpful by 7% and not helpful by 3%. In-depth guidance on how to comply with different requirements of the AI Act (e.g. for high-risk AI Systems; Risk Management system, Fundamental Rights Impact Assessment...) was seen as very helpful by 30% of respondents, extremely helpful by 27%, helpful by 21%, and slightly helpful by 10%. No one rated this to be not helpful. Evaluating my compliance with the AI Act was viewed as extremely helpful by 33% of respondents, helpful by 25%, very helpful by 19%, slightly helpful by 9% and not helpful by 1% of respondents.

36% of respondents said that they viewed identification, assessment, management, and (guidance on) ongoing monitoring of AI risks, in compliance with the AI Act as helpful, 31% as very helpful, 13% as extremely helpful, 6% as slightly helpful and 1% as not helpful. Staying in contact with authorities was rated very helpful by 22% of respondents, helpful by another 22%, slightly helpful by 19%, extremely helpful by 13% and not helpful by 10% of respondents. Receiving clear guidance from authorities on how to comply with the GDPR and related data requirements was viewed as very helpful by 33% of respondents, helpful by 27%, extremely helpful by 13%, slightly helpful by 9% and not helpful by 6% of respondents. 28% of respondents rated navigating the intersection between different laws as extremely helpful, 24% as very helpful, 22% as helpful, 10% as slightly helpful and 3% as not helpful. The median and mode values of the responses were also calculated and presented in the following figure, and the distribution of answers is presented in the following graph.

	Identifying the risk level, including high-risk systems, of my AI technologies, as per the AI Act	General guidance on how to comply with the AI Act	In-depth guidance on how to comply with different requirements of the AI Act (e.g. for high-risk AI Systems; Risk Management system, Fundamental Rights Impact Assessment...)	Evaluating my compliance with the AI Act	Identification, assessment, management, and (guidance on) ongoing monitoring of AI risks, in compliance with the AI Act	Staying in contact with authorities	Receiving clear guidance from authorities on how to comply with the GDPR and related data requirements	Navigating the intersection between different laws
Median	3	4	4	4	4	3	4	4
Mode	3	4	4	5	3	3	4	5

Figure 23. Median and mode of responses to the question regarding how helpful the respondents viewed different mechanisms of the regulatory sandbox

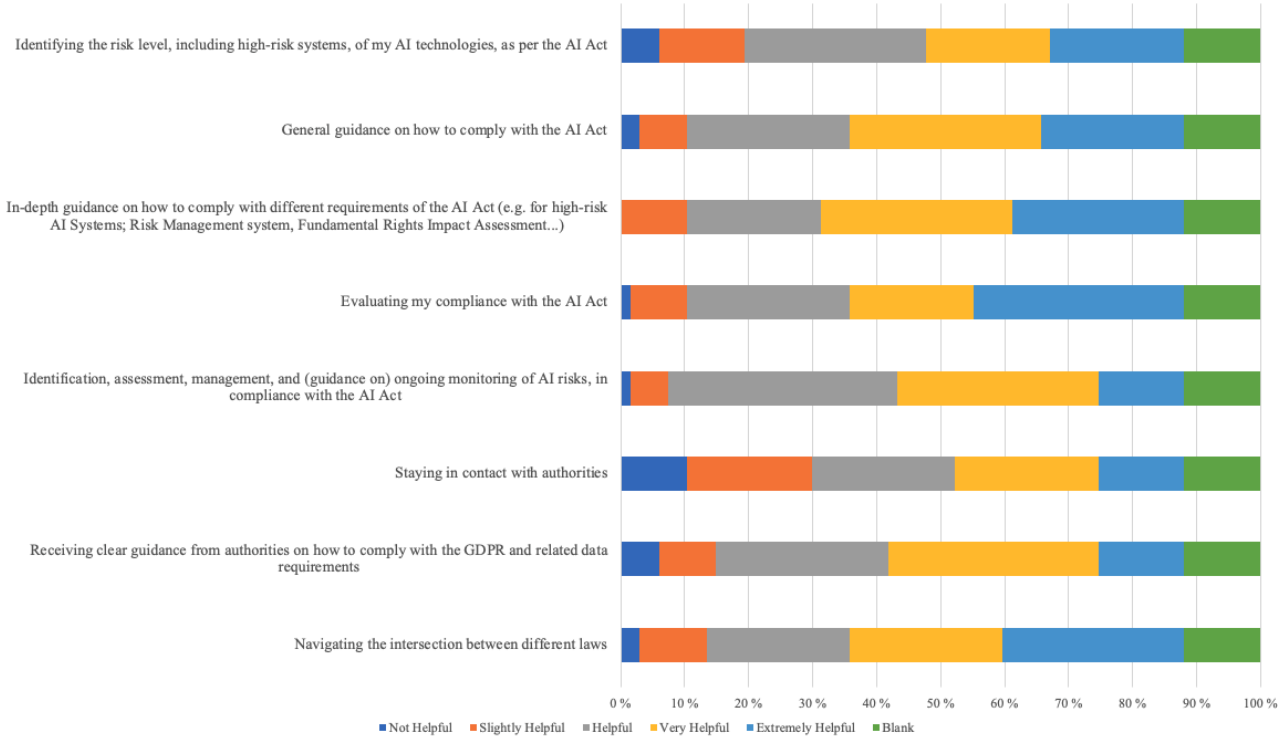

Figure 24. Distribution of responses to the question regarding how helpful the respondents viewed different mechanisms of the regulatory sandbox

12 respondents had also openly told some other mechanisms they would see helpful for their organisation's participation in a sandbox and some common themes were reduce the cost of training, identify future needs and improvements and gain and improve customers' trust.

Four mechanisms that were rated extremely helpful and very helpful the most were in-depth guidance on how to comply with different requirements of the AI Act, general guidance on how to comply with the AI Act, evaluating my compliance with the AI Act and navigating the intersection

between different laws and the mechanism rated least helpful out of all of them was staying in contact with the authorities.

Next, the participants were presented with different areas to save time when participating in a sandbox and asked to select one or more areas they would expect to save time. The areas were: legal compliance, time to market, developing your AI technology, training your AI technology, testing your AI technology, validating your AI technology and understanding the compliance with the AI Act. This question was answered by 58 respondents. Most selected area was legal compliance, selected by 70% of respondents, understanding the compliance with the AI Act was selected by 58%, validating your AI technology by 45%, testing your AI technology by 40%, time to market by 34%, developing your AI technology by 28% and training your AI technology by 25% of respondents. One respondent had also answered that their organisation expected to save time in finding new customers. Based on these respondents' answers, most companies expect to save time with issues related to regulatory compliance.

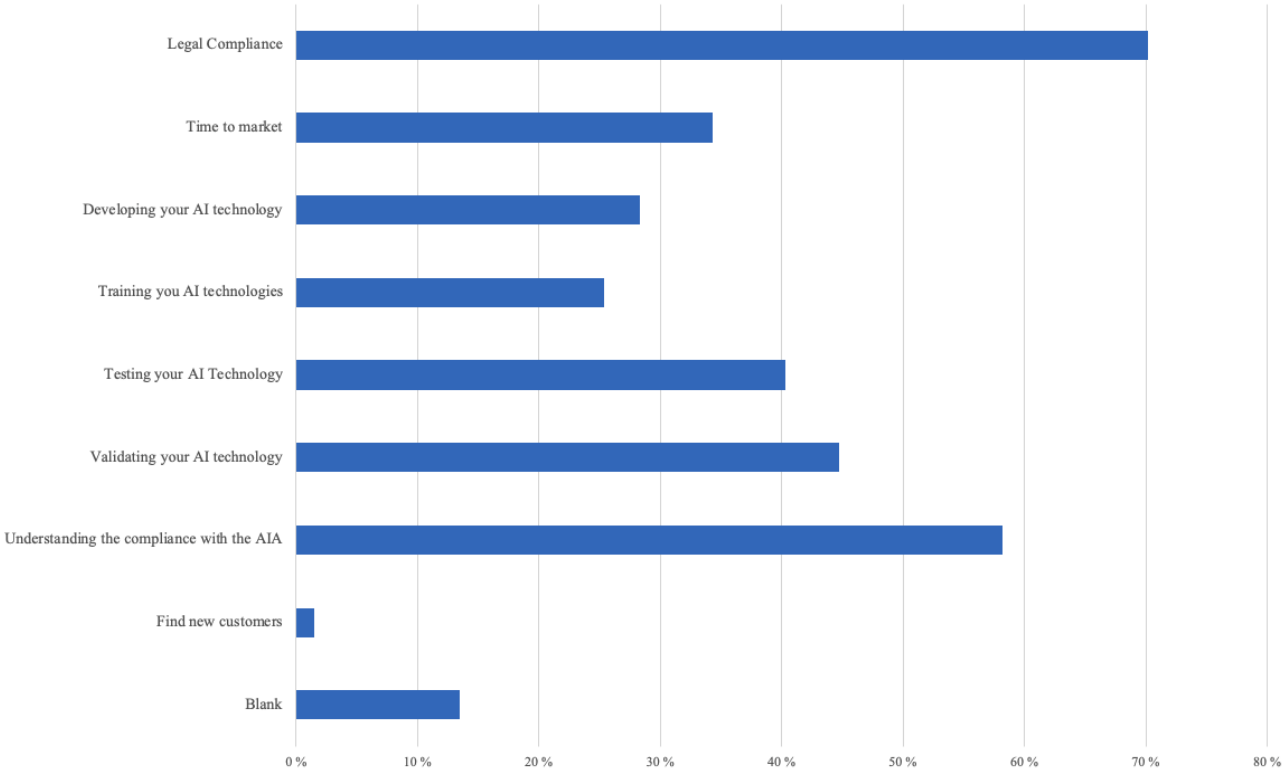

Figure 25. Distribution of responses to the question regarding which areas the respondents would expect to save time when participating in a regulatory sandbox

The respondents were then asked how much time they expected to save based on their selections in the previous question. Most respondents (34%) reported that they expected to save 1–3 months.

16% also reported that they expected to save 3–6 months, 13% less than one month and 12% expected to save 6–12 months. Only four companies expected to save more than a year of time.

Lastly, the respondents were asked if they were willing to cover any costs for their participation in the sandbox and if yes, how much. Majority of the respondents (64%) said that they would not be willing to cover any costs for their sandbox participation and only 24% of respondents said yes, they would be willing to cover partially or fully the cost of their participation in the sandbox. Seven companies that were willing to cover any costs reported that they would be willing to cover 1000–5000 euros, five companies were willing to cover maximum of 500 euros, two companies 10000 euros, one company 20000 euros and one company 300000 euros.

8 Conclusions

8.1 Conclusion

The development and use of artificial intelligence systems is increasing and so is the concern about how these systems and AI as a whole, could negatively impact individuals and societies. Consequently, many actors such as the European Union have placed focus on AI regulation and how to safely develop new AI systems so that they would not compromise individuals' fundamental rights or democratic societies. Small and medium-sized enterprises make up a large portion of the European economy and the EU has thus placed increased focus on helping them in AI development. The aim of this thesis is to map out how the AI regulatory sandboxes presented in the new EU regulatory framework for AI, the EU AI Act, could affect development of AI and AI innovation in small and medium-sized enterprises. In order to meet the stated objective of this thesis, the main research question was stated:

RQ: What possible effects could the AI regulatory sandbox have on AI development in SMEs?

Additionally, two auxiliary research questions were stated:

ARQ1: What possible challenges could SMEs face in accessing and utilizing sandbox models effectively?

ARQ2: What specific tools and support can sandboxes offer to SMEs?

AI regulatory sandboxes are a very new approach used in artificial intelligence regulation and there are not yet public results from any AI Act regulatory sandboxes. Currently there is only one AI regulatory sandbox that is done in collaboration with the AI Act, the Spanish sandbox presented earlier in this thesis. However, currently there are no publicly available exit reports from the sandbox, thus, the effectiveness of the AI Act regulatory sandboxes cannot yet be studied. Regulatory sandboxes, however, have been utilised in other sectors such as fintech and privacy, and especially in fintech they have been relatively successful for stakeholders involved. For SMEs, the fintech regulatory sandboxes have offered many benefits such as reduced time to market, increased investment, increased innovation, facilitated market entry, access to regulatory guidance and help in understanding regulations better. The privacy sandboxes have also offered benefits such as reduced time to market for participating companies. The regulatory sandboxes, however, have had some challenges such as vague selection criteria and unclear regulatory authority and they pose potential risks such as potential discrimination and damage to competition if not designed and monitored

properly. AI is nonetheless very different from financial technology and privacy related technology, and it poses unique risks and challenges that have to be considered when regulating it. Thus, the results from fintech and privacy sandboxes cannot directly be applied to AI. The benefits and challenges of existing regulatory sandboxes are presented to show what kind of effects regulatory sandboxes can have when applied to any regulatory framework.

The empirical part of this thesis was done as survey research as there were two questionnaires available to use in this thesis that were done as a part of the project EUSAiR. The data was collected through the two questionnaires, and they were available for answering on the internet. The data from the questionnaires was analysed using descriptive statistics and the results were presented following the modified TOE framework selected for this thesis.

After the methodology chapter, the results of the questionnaires were presented. The results were calculated using descriptive statistics to describe the overall views of the participants. For this thesis, the most important questionnaire questions were those that covered SMEs attitudes towards regulation, especially AI regulation, and the AI regulatory sandbox. Following the framework for this thesis it can be identified that environmental factors, in this instance, regulation, does affect the AI development and deployment to at least some degree. The AI regulatory sandbox and its aspects presented in the questionnaires were mainly viewed as important and useful to the organisation.

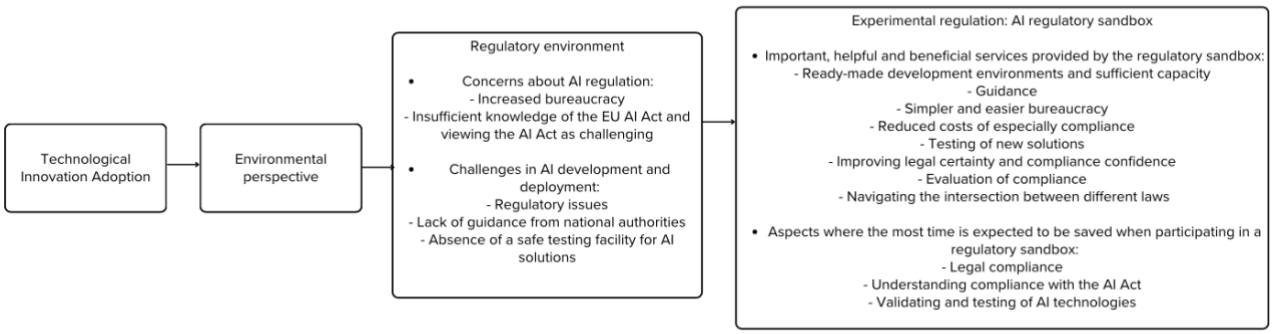

Figure 26. The effects of regulatory environment and experimental regulation to technological adoption in SMEs

To answer the main research question RQ: What possible effects could the AI regulatory sandbox have on AI development in SMEs? The AI regulatory sandbox could help SMEs navigate the regulatory environment surrounding AI better and consequently help them develop more trustworthy and compliant AI solutions. The regulatory sandbox can offer guidance and help regarding the concerns about AI regulation that SMEs have such as insufficient knowledge and increased bureaucracy. Additionally, the AI regulatory sandbox can help SMEs tackle the current

challenges in their AI development and deployment such as regulatory issues, lack of guidance and absence of a safe testing facility for AI solutions. Based on the results of the questionnaires the AI regulatory sandbox could also help SMEs save time in various aspects of AI development such as legal compliance and understanding compliance with the AI Act as well as validating and testing of AI technologies.

The first auxiliary research question ARQ1 regarded the challenges of AI regulatory sandboxes and to answer this the cost of participating in a regulatory sandbox would be an issue for most SMEs. However, in the AI Act it is stated that SMEs would be able to utilise the sandbox for free, thus this should solve the issue of cost. Other issues and challenges that were openly mentioned in the questionnaires were lack of harmonised standards and the possibility of the sandbox becoming too bureaucratic.

To answer the second auxiliary research question ARQ2: The AI regulatory sandbox can offer tools and support to SMEs such as a ready-made and safe environment to develop test and validate AI technologies and regulatory guidance as well as specific guidance on how to comply with the AI Act. The regulatory sandbox also offers a safe space for cooperation with AI Act supervisory authorities and for evaluation of compliance. Reduced costs and easier bureaucracy are additionally offered by the regulatory sandbox.

8.2 Discussion and contributions

The AI regulatory sandbox is a quite new phenomenon and thus there is not sufficient prior research done on them to reflect the findings of this thesis. As mentioned previously in this thesis currently the Spanish regulatory sandbox is the only one done in collaboration with the EU AI Act and there are no publicly available reports from it yet. However, there have been regulatory sandboxes in other industries such as fintech and privacy and the findings from these have been documented. It is important to note that artificial intelligence and financial technology and privacy cannot be directly compared and the regulatory environment surrounding them is not the same. This is mind, there are similarities between the documented results of the fintech and privacy sandboxes and findings from this study regarding the attitudes towards AI regulatory sandboxes.

Existing regulatory sandboxes have been shown to promote innovation, and the AI regulatory sandboxes offer a space for testing new solutions which has the potential to promote innovation. Access to regulatory guidance and better understanding of regulations as well as reduced costs are also shown to be a benefit of the existing regulatory sandboxes, and these are also viewed as a

potential and important benefits of the AI regulatory sandbox. The AI regulatory sandbox offers a space where authorities are in the same place, and this has the potential to improve communication between stakeholders which is also a benefit offered by the existing regulatory sandboxes.

The fintech and privacy sandboxes have offered benefits such as reduced time to market, increased investment and facilitated market entry for companies, but it cannot yet be verified if the AI regulatory sandbox can offer these same benefits. The AI regulatory sandbox is anticipated to ease the bureaucratic processes concerning regulation, but this is not directly shown to be a benefit of the existing regulatory sandboxes. These are, however, shown to help companies interpret regulations better.

Regarding the challenges and risks of the fintech and privacy sandboxes there have been mentions of fragmented regulation and lack of harmonised regulatory frameworks and these were mentioned to be potential challenges of the AI regulatory sandboxes as well. There has been discussion around the risks of regulatory sandboxes if they are designed insufficiently and if the selection criteria are not adequately defined. These risks include damage to competition and stakeholders. These risks were not mentioned in the questionnaires but are still important to consider when it comes to the design of AI regulatory sandboxes.

The design of the questionnaires used in this thesis guided the respondents quite significantly since the questionnaires were mainly multiple selection questions and questions utilising the Likert scale. The respondents were able to provide their own open answers to some of the questions but for most questions this was not the case. The questionnaires also only gathered the attitudes of the respondents towards AI regulation and AI regulatory sandboxes, thus any concrete data from the AI regulatory sandboxes was not obtained.

8.3 Limitations and future research

The chosen empirical method of this thesis poses this thesis to some limitations. The empirical part was done as survey research, and the design of the data collection method limited the possibility of different answers that the respondents could give. Additionally, there is no certainty that the respondents knew the definitions of some of the terms used in the questions. For example, the different risk categories in the AI Act and the regulatory sandbox itself may not have been sufficiently familiar to the respondents. Furthermore, respondents may interpret the options on a Likert scale differently. Also, the framework used in this thesis does not consider the technological and organisational aspects of AI development and technological innovation in SMEs, and to get a

comprehensive picture of factors affecting AI development and innovation the results of this thesis would need to be adequately scaled and compared to the technological and organisational aspects.

The data analysis in this thesis was only done using descriptive statistics and not inferential statistics. It is possible that there could be additional results obtained through hypothesis testing, however, in the data used in this thesis there were no clear groups that could be compared to each other or the relationships between them could be tested.

The majority of respondents of the questionnaires were mostly from Finland and Italy and for future research it could be beneficial to collect more data from other countries as well. Additionally, as there is not real data from the AI regulatory sandboxes yet, this topic can be more profoundly explored when there are sufficientt results from these sandboxes. This thesis has the possibility to offer support in the development and design of the AI regulatory sandboxes and can be utilised as a basis for future research on this topic.

References

AFM & DNB, (2019). Continuing dialogue - InnovationHub and Regulatory Sandbox: lessons learned after three years. <Continuing dialogueAFM.nlhttps://www.afm.nl › innovationhub-rapport-eng>, retrieved 28.4.2025.

Ahern, D. (2021). Regulatory lag, regulatory friction and regulatory transition as fintech disenablers: Calibrating an EU response to the regulatory sandbox phenomenon. European Business Organization Law Review, Vol. 22, 395–432. https://doi.org/10.1007/s40804-021-00217-z.

Attrey, A., Lesher, M. & Lomax, C. (2020). The role of sandboxes in promoting flexibility and innovation in the digital age. OECD Going Digital Toolkit Notes, No. 2, OECD Publishing, Paris, https://doi.org/10.1787/cdf5ed45-en.

Bagni, F. (2025). Regulatory Sandboxes as a bridge between AI and cybersecurity: Exploring the interplay between the AI Act and the Cyber Resilience Act. In: Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders, eds. Bagni, F. & Seferi, F. 54–69. CINI's Cybersecurity National Lab. ISBN: 9788894137378.

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. Harvard Journal of Law & Technology, Vol. 31 (2), 889–938.

BIAC, (2020). Regulatory Sandboxes for privacy analytical report. <https://25159535.fs1.hubspotusercontent-eu1.net/hubfs/25159535/website/documents/pdf/Digital%20Economy/Regulatory%20Sandboxes%20for%20Privacy%20-%20Analytical%20Report.pdf>, retrieved 28.4.2025.

Black, J. & Murray, A. D. (2019). Regulating AI and machine learning: Setting the regulatory agenda. European Journal of Law and Technology, Vol. 10 (3).

BMWi, (2019). Making space for innovation – The handbook for regulatory sandboxes. Federal Ministry for Economic Affairs and Energy (BMWi), Public Relations, Berlin. <https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory-sandboxes.pdf?__blob=publicationFile&v=2>, retrieved 9.5.2025.

Bradford, A. (2024). The false choice between digital regulation and innovation. Northwestern University Law Review, Vol. 119 (2), 377–454.

Brodny, J. & Tutak, M. (2022). Digitalization of small and medium-sized enterprises and economic growth: Evidence for the EU-27 countries. Journal of Open Innovation: Technology, Market, and Complexity, Vol. 8 (2), 67. https://doi.org/10.3390/joitmc8020067.

Buckley, R. P., Arner, D., Veidt, R. & Zetzsche, D. (2020). Building fintech ecosystems: Regulatory sandboxes, innovation hubs and beyond. Washington University Journal of Law & Policy, Vol. 61, 55–98.

Business Software Alliance, (2023). AI Developers and deployers: An important distinction. <https://www.bsa.org/files/policy-filings/03162023aidevdep.pdf>, retrieved 24.6.2025.

Caruana, M. M. & Borg, R. M. (2024). Regulating artificial intelligence in the European Union. In: The EU internal market in the next decade–Quo Vadis?, eds. Sammut, I. & Mifsud, I., 108–142. Koninklijke Brill BV, Leiden.

Chatterjee, S., Chaudhuri, R., Vrontis, D. & Basile, G. (2022). Digital transformation and entrepreneurship process in SMEs of India: A moderating role of adoption of AI-CRM capability and strategic planning. Journal of Strategy and Management, Vol. 15 (3), 416–433. https://doi.org/10.1108/JSMA-02-2021-0049.

Chen, H., Li, L. & Chen, Y. (2020). Explore success factors that impact artificial intelligence adoption on telecom industry in China. Journal of Management Analytics, Vol. 8 (1), 36–68. https://doi.org/10.1080/23270012.2020.1852895.

Crockett, K., Colyer, E., Gerber, L. & Latham, A. (2023). Building trustworthy AI solutions: A case for practical solutions for small businesses. IEEE Transactions on Artificial Intelligence, Vol. 4 (4), 778–791. doi: 10.1109/TAI.2021.3137091.

Dardykina, A. (2026). Is there enough sand in the sandbox? Forthcoming in the European Business Law Review. ONKO OIKEIN?

Datatilsynet, (2023). Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence. <https://www.datatilsynet.no/contentassets/41e268e72f7c48d6b0a177156a815c5b/agenda-kaupang-evaluation-sandbox_english_ao.pdf>, retrieved 9.5.2025.

DIGITAL, The Digital Europe Programme. <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>, retrieved 1.6.2025.

Draghi, M. (2024). The future of European competitiveness: A competitiveness strategy for Europe (Part A), <https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf>, retrieved 5.2.2025.

EC-OECD, (2025), STIP Compass: International Database on Science, Technology and Innovation Policy (STIP), edition June 24, 2025, https://stip.oecd.org.

El-Haddadeh, R. (2020). Digital innovation dynamics influence on organisational adoption: The case of cloud computing services. Information Systems Frontiers, Vol. 22, 985–999. https://doi.org/10.1007/s10796-019-09912-2.

El-Haddadeh, R., Osmani, M., Hindi, N. & Fadlalla, A. (2021). Value creation for realising the sustainable development goals: Fostering organisational adoption of big data analytics. Journal of Business Research, Vol. 131, 402–410. https://doi.org/10.1016/j.jbusres.2020.10.066.

ESMA, EBA, EIOPA, (2018). Fintech: Regulatory sandboxes and innovation hubs, <https://www.esma.europa.eu/sites/default/files/library/jc_2018_74_joint_report_on_regulatory_sandboxes_and_innovation_hubs.pdf>, retrieved 9.5.2025.

EU, (2024). Regulation (EU) 2024/1689. Official Journal of the European Union, L series.

EU AI Act High Level Summary. <https://artificialintelligenceact.eu/high-level-summary/>, retrieved 10.2.2025.

European Commission: SME definition. <https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en>, retrieved 23.11.2024.

European Commission (2019a). Expert Group on regulatory obstacles for financial innovation (ROFIEG). <https://finance.ec.europa.eu/document/download/98a331c4-6700-4355-b545-cb97a49f13c2_en?filename=191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf>, retrieved 10.2.2025.

European Commission, (2019b). High-Level Expert Group on Artificial Intelligence (HLEG), A Definition of AI: Main Capabilities and Disciplines, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>, retrieved 3.4.2025.

European Commission, (2023). Better Regulation Toolbox 2023. Chapter 8 – Methodologies for analysing impacts in impact assessments, evaluations, and fitness checks. <https://commission.europa.eu/document/download/0d32ee11-92da-434d-9c86-fd4579d95dc6_en?filename=BRT-2023-Chapter%208-Methodologies%20for%20analysing%20impacts%20in%20IAs%20evaluations%20and%20fitness%20checks_0.pdf>, retrieved 24.11.2024.

EUSAiR, (2024). Supporting the establishment of AI regulatory sandboxes across the EU in alignment with the AI Act requirements. EU Digital Europe Supporting Action, GAP-101195535, 1.12.2024– 31.12.2026. https://eusair-project.eu.

financial technology (fintect). 2025. In *Cambridge Dictionary*. <https://dictionary.cambridge.org/dictionary/english/financial-technology>, retrieved 24.6.2025.

Glasow, P. A. (2005). *Fundamentals of survey research methodology*. MITRE, Washington C3 Center. McLean, Virginia.

Goo, J. J. & Heo, JY. (2020). The impact of the regulatory sandbox on the fintech industry, with a discussion on the relation between regulatory sandboxes and open innovation. Journal of Open Innovation: Technology, Market, and Complexity, Vol. 6 (2), 43. https://doi.org/10.3390/joitmc6020043.

Ho, C.WL. & Caals, K. (2024). How the EU AI Act seeks to establish an epistemic environment of trust. Asian Bioethics Review, Vol. 16, 345–372. https://doi.org/10.1007/s41649-024-00304-6.

Horváth, D. & Szabó, R., Z. (2019). Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities? Technological Forecast and Social Change, Vol. 146, 119–132. https://doi.org/10.1016/j.techfore.2019.05.021.

Huiping, W. & Leung, S. O. (2017). Can a Likert scale be treated as interval scales? – A simulation study. Journal of Social Service Research, Vol. 43 (4), 527–532. http://dx.doi.org/10.1080/01488376.2017.1329775.

Ingaldi, M. & Ulewicz, R. (2020). Problems with the implementation of Industry 4.0 in enterprises from the SME sector. Sustainability, Vol. 12 (1), 217. https://doi.org/10.3390/su12010217.

innovation. 2025. In *Cambridge Dictionary*. <https://dictionary.cambridge.org/dictionary/english/innovation>, retrieved 24.6.2025.

Iyelolu, T., V., Agu, E., E., Idemudia, C. & Ijomah, T., I. (2024). Driving SME innovation with AI solutions: overcoming adoption barriers and future growth opportunities. International Journal of Science and Technology Research Archive, Vol. 7 (1), 36–54. https://doi.org/10.53771/ijstra.2024.7.1.0055.

Jafarzadeh, P., Vähämäki, T., Nevalainen, P., Tuomisto, A. & Heikkonen, J. (2024). Supporting SME companies in mapping out AI potential: a Finnish AI development case. The Journal of Technology Transfer. https://doi.org/10.1007/s10961-024-10122-5.

Jöhnk, J., Weißert, M. & Wyrtki, K. (2021). Ready or not, AI comes — An interview study of organizational AI readiness factors. Business & Information Systems Engineering, Vol. 63, 5–20. https://doi.org/10.1007/s12599-020-00676-7.

Keiding, N. & Louis, T., A. (2018). Web-based enrollment and other types of self-selection in surveys and studies: Consequences for generalizability. Annual Review of Statistics and Its Applications, Vol. 5, 25–47. https://doi.org/10.1146/annurev-statistics- 031017- 100127.

Likert, R. (1932). A technique for the measurement of attitudes. Archives of Psychology, 22 140, 55.

Madiega, T. & De Pol, A., L., Van (2022). Artificial intelligence act and regulatory sandboxes. European Parliamentary Research Service (EPRS). <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf>, retrieved 26.11.2024.

Mahroof, K. (2019). A human-centric perspective exploring the readiness towards smart warehousing: The case of a large retail distribution warehouse. International Journal of Information Management, Vol. 45, 176-190. https://doi.org/10.1016/j.ijinfomgt.2018.11.008.

Moraes, T. (2024). Ethical AI regulatory sandboxes: Insights from cyberspace regulation and internet governance. In: Proceedings of the Second International Symposium on Trustworthy Autonomous Systems (TAS '24), Article 17, 1–10. Association for Computing Machinery, New York. https://doi.org/10.1145/3686038.3686049.

Moses, L., B. (2011). Agents of change: How the law 'copes' with technological change. Griffith Law Review, Vol. 20 (4),764–794.

Moses, L., B. (2013). How to think about law, regulation and technology: Problems with "technology" as a regulatory target. Law, Innovation & Technology, Vol. 5 (1), 1–20. DOI: 10.5235/17579961.5.1.1.

Muminova, E., Ashurov, M., Akhunova, S. & Turgunov, M. (2024). AI in small and medium enterprises: Assessing the barriers, benefits, and socioeconomic impacts. International Conference on Knowledge Engineering and Communication Systems (ICKECS), 1–6. Chikkaballapur, India. doi: 10.1109/ICKECS61492.2024.10616816.

Müller, J., M., Buliga, O. & Voigt, KI. (2018). Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0, Technological Forecasting and Social Change, Vol. 132, 2–17. https://doi.org/10.1016/j.techfore.2017.12.019.

OECD, (2019). AI Principles overview. <https://oecd.ai/en/ai-principles>, retrieved 11.4.2025.

OECD, (2021), State of implementation of the OECD AI Principles – Insights from national AI policies. OECD Digital Economy Papers, 311. OECD Publishing, Paris, https://doi.org/10.1787/1cd40c44-en.

OECD, (2023). Regulatory sandboxes in artificial intelligence. OECD Digital Economy Papers, 356. OECD Publishing, Paris, https://doi.org/10.1787/8f80a0e6-en.

Oldendick, R. W. (2012). Survey research ethics. In: Handbook of survey methodology for the social sciences, eds. Gideon, L. Springer, New York. https://doi.org/10.1007/978-1-4614-3876-2_3.

Olsen, B. (2020). Sandbox for responsible artificial intelligence, <https://dataethics.eu/sandbox-for-responsible-artificial-intelligence/>, retrieved 28.4.2025.

Omrani, N., Rejeb, N., Maalaoui, A., Dabić, M. & Kraus, S. (2022). Drivers of digital transformation in SMEs. IEEE Transactions on Engineering Management, Vol. 71, 5030–5043. doi: 10.1109/TEM.2022.3215727.

Paré, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, Vol. 52 (2), 183–199.

Parenti, R. (2020). Regulatory sandboxes and innovation hubs for fintech: Impact on innovation, financial stability and supervisory convergence. Study for the Committee on Economic and Monetary Affairs, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, Cambridge, MA and London. https://doi.org/10.4159/harvard.9780674736061.

Pošćić, A. & Martinović, A. (2022). Regulatory Sandboxes under the Draft EU Artificial Intelligence Act: An Opportunity for SMEs? Journal for the international and European law, economics and market integrations, Vol. 9 (2), 71–117. https://doi.org/10.22598/iele.2022.9.2.3.

Ranchordás, S. (2021). Experimental regulations for AI: Sandboxes for morals and mores. University of Groningen Faculty of Law Research Paper No. 7/2021, Groningen. http://dx.doi.org/10.2139/ssrn.3839744.

Regulation. 2025. In *Cambridge Dictionary*. <https://dictionary.cambridge.org/dictionary/english/regulation>, retrieved 24.6.2025.

Ruschemeier, H. (2025). Thinking outside the box? In: Bridging the gap between AI and reality. AISoLA 2023. Lecture Notes in Computer Science, eds. Steffen, B. 14129. Springer, Cham. https://doi.org/10.1007/978-3-031-73741-1_20.

Schwaeke, J., Peters, A., Kanbach, D., K., Kraus, S., & Jones, P. (2024). The new normal: The status quo of AI adoption in SMEs. Journal of Small Business Management, Vol. 63 (3), 1297–1331. https://doi.org/10.1080/00472778.2024.2379999.

Sima, V., Gheorghe, I. G., Subić, J. & Nancu, D. (2020). Influences of the Industry 4.0 revolution on the human capital development and consumer behavior: A systematic review. Sustainability, Vol. 12 (10), 4035. https://doi.org/10.3390/su12104035.

Sky, N. (2024). Systematic review of regulatory Sandboxes: implications for the European Union's Artificial Intelligence Act. Master's Thesis. University of Oulu. https://urn.fi/URN:NBN:fi:oulu-202406194763.

Sloane, M. & Wüllhorst, E. (2025). A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada. Data & Policy, Vol. 7, e11. doi:10.1017/dap.2024.54.

The Future Society, (2022). Sandboxes without the quicksand: making EU AI sandboxing work for regulators, entrepreneurs and society. Memo by the Future Society (TFS), <https://thefuturesociety.org/wp-content/uploads/2022/06/Sandboxes-without-the-quicksand.pdf>, retrieved 5.2.2025.

Timan, T., Oirsouw, C., van & Hoekstra, M. (2021). The role of data regulation in shaping AI: an overview of challenges and recommendations for SMEs. In: The Elements of Big Data Value, eds. Curry, E., Metzger, A., Zillner, S., Pazzaglia, JC. & García Robles, A., 355–376. Springer Nature Switzerland AG, Cham. https://doi.org/10.1007/978-3-030-68176-0.

Tornatzky, L. G. & Fleischer, M. (1990). The processes of technological innovation. Lexington Books, Lexington.

Truby, J., Brown, R. D., Ibrahim, I. A. & Parellada, O. C. (2021). A Sandbox approach to regulating high-risk artificial intelligence applications. European Journal of Risk Regulation, Vol. 13 (2), 270–294. doi:10.1017/err.2021.52.

Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI. European Papers – A Journal on Law and Integration, European Forum, Insight, Vol. 5 (2), 1087-1097. doi: 10.15166/2499-8249/394.

U.K. Government, (2019). Understanding artificial intelligence ethics and safety. <https://www.gov.uk/guidance/understanding-artificial-intelligence-ethics-and-safety>, retrieved 9.5.2025.

UNESCO, (2021). Draft text of the recommendation on the ethics of artificial intelligence. <https://unesdoc.unesco.org/ark:/48223/pf0000377897>, retrieved 9.5.2025.

UNESCO, (2022). Recommendation on the Ethics of Artificial Intelligence. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>, retrieved 11.4.2025.

U.S. Government, (2020). Guidance for regulation of artificial intelligence applications. <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>, retrieved 9.5.2025.

Wei, R. & Pardo, C. (2022). Artificial intelligence and SMEs: How can B2B SMEs leverage AI platforms to integrate AI technologies? Industrial Marketing Management, Vol. 107, 466–483. https://doi.org/10.1016/j.indmarman.2022.10.008.

Williamsson, K. & Johanson, G. C. (2017). Research methods: Information, Systems and Contexts. Chandos Publishing, Cambridge & Kidlington.

Wolf-Brenner, C., Pammer-Schindler, V. & Breitfuss, G. (2024). How do professionals in SMEs engage with AI and regulation? An interview study in Austria. In: Proceedings of Mensch und Computer 2024 (MuC '24), eds. Maedche, A. & Beigl, M., 646–650. Association for Computing Machinery, New York. https://doi.org/10.1145/3670653.3677514.

World Bank, (2020). Global Experiences from Regulatory Sandboxes. Fintech Note;No. 8. © World Bank. http://hdl.handle.net/10986/34789. License: CC BY 3.0 IGO.

Zarra, A. (2025). Operationalizing AI regulatory sandboxes: A look at the incentives for participating start-ups and SMEs beyond compliance. In: Regulatory sandboxes for AI and Cybersecurity. Questions and answers for stakeholders, eds. Bagni, F. & Seferi, F. 101–115. CINI's Cybersecurity National Lab. ISBN: 9788894137378.

Zetzsche, D., A., Buckley, R., P., Barberis, J., N. & Arner, D., W. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. Fordham Journal of Corporate & Financial Law, Vol. 23 (1), 2.

Appendices

Appendix 1: Research data management plan for students

Eeva Kaakkurivaara

Research data

Research data type	Contains personal details/information*	I will gather/produce the data myself	Someone else has gathered/produced the data	Other notes
Data type 1: *2024 questionnaire excel file*			x	
Data type 2: *2025 questionnaire excel file*	x		x	

* Personal details/information are all information based on which a person can be identified directly or indirectly, for example by connecting a specific piece of data to another, which makes identification possible. For more information about what data is considered personal go to the Office of the Finnish Data Protection Ombudsman's website

Processing personal data in research

I will prepare a Data Protection Notice** and give it to the research participants before collecting data ☐

The controller** for the personal details is the student themself ☒ the university ☐

My data does not contain any personal data ☐

** More information at the university's intranet page, Data Protection Guideline for Thesis Research

Permissions and rights related to the use of data

Self-collected data

This thesis does not contain self-collected data.

Data collected by someone else

Rights and licences related to the data

Data was collected by Haaga-Helia and ALLAI for the EUSAiR project and it is available for use among the project participants. EUSAiR project coordinator the University of Bologna and ALLAI have shared the data with the project participants.

Data type 1: 2024 questionnaire excel file

Data type 2: 2025 questionnaire excel file

Storing the data during the research process

Where will you store your data during the research process?

In the university's network drive ☐
In the university-provided Seafile Cloud Service ☐
Other location, my own personal computer: ☒

The data is stored on my personal computer, and I have taken care of the necessary file backups. The computer is not accessible by anyone else, and thus the data is stored securely.

Documenting the data and metadata

Data documentation

To document the data, I will use:

A field/research journal ☐

A separate document where I will record the main points of the data, such as changes made, phases of analysis, and significance of variables ☒

A readme file linked to the data that describes the main points of the data ☐

Other, please specify: ☐

Data arrangement and integrity

I will keep the original data files separate from the data I am using in the research process, so that I can always revert back to the original, if need be. ☒

Version control: I will plan before starting the research how I will name the different data versions and I will adhere to the plan consistently. ☒

I recognise the life span of the data from the beginning of the research and am already prepared for situations, where the data can alter unnoticed, for example while recording, transcribing, downloading, or in data conversions from one file format to another, etc. ☒

Metadata

Metadata is a description of you research data. Based on metadata someone unfamiliar with your data will understand what it consists of.

I will save my data into an archive or a repository that will take care of the metadata for me. ☐

I will have to create the metadata myself, because the archive/repository where I am uploading the data requires it. ☐

I will not store my data into a public archive/repository, and therefore I will not need to create any metadata. ☒

Data after completing the research

I will handle the data according to the agreements I have made. The university recommends a general retention period of five years, with an exception for medical research data, where the retention period is 15 years. Personal data can only be stored as long as it is necessary. If you have agreed to destroy the data after a set time period, you are responsible for destroying the data, even if you no longer are a student at the university. Likewise, when using the university's online storage services, destroying the data is your responsibility.
After this thesis is completed, I will no longer participate in the EUSAiR project, and I will return the data to project which is then responsible for it.

This data management plan is updated throughout the research project.