The effects of recent EU regulations on software development

University of Turku
Master of Science (Tech) Thesis
Department of Computing
Software engineering
2025
Eemeli Tynys

UNIVERSITY OF TURKU
Department of Computing

Eemeli Tynys: The effects of recent EU regulations on software development

Master of Science (Tech) Thesis, 68 p., 8 app. p.
Software engineering
May 2025

European Union (EU) has increased its presence in the field of software development with the adoption of the Digital Decade program. The goal of EU is to make EU citizens more proficient with digital technologies and make sure that companies develop new systems using the latest technologies whilst being responsible with that technology and the data that they collect from the EU citizens.
This thesis set out to find what changes recent EU regulations like GDPR (General Data Protection Regulation), DORA (Digital Operational Resilience Act) and AI (Artificial Intelligence) Act have caused to software development and how these necessary changes can be accomplished. This thesis used literary review and interviews as research methods. GDPR and the AI Act were reviewed and a list of requirements were formed based on them. The requirements were categorised into two different categories based on if they affect more the developed system, or the development process itself. The interviews were conducted in a semi-structured manner where the list of requirements was also provided to the interviewees and they were asked about the different requirements.
It was found that software developers need to create systems and practises that have previously been considered good practises, as they have been included in the recent regulations as mandatory. Literary analysis also found that developers need to be aware at all times, what the developed systems are capable of, and they need to communicate to the users what the intended use cases are.
The interviews confirmed these findings and also noted, that EU seems to include similar requirements in different regulations. The process of adopting new techniques and methods is complex and companies need to start the preparation process for the adoption of the regulations early. Without coordination within the company, the adoption of regulations can be become much more difficult as without it different teams try to solve the same problems, which would lead to unnecessary conflicts.

Keywords: software development, GDPR, DORA, AI Act, European Union

Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The European Union (EU) launched the *Digital Decade* program in 2022 as the latest program to develop the digital skills of the EU citizens, to improve the adaption of new technologies, to advance the connectivity and data infrastructure in the EU, and to make public services and administration available online. [1] This reflects the current motivation for the EU to become a more digital society, where IT-related companies can flourish and offer meaningful services to companies and citizens alike.

One aspect of achieving this goal is regulating software development, which EU has started to increasingly regulate with legislation like the *General Data Protection Regulation* (GDPR) [2] and the *Artificial Intelligence Act* (AI Act) [3]. This increase in the amount of legislation puts pressure on the companies that develop software to prepare and predict, what changes they need to make in order to stay compliant with the regulations.

EU has increasingly included things that have been previously self-monitored by the developers as good practises and codes of conduct in the newer regulations. [4] This has hardened the EU´s stance on how software has to be developed and what quality requirements the finished product has to have in order to be compliant with regulations.

1.2 Thesis goals and research questions

The goal of this thesis is to analyse the recent EU regulations and analyse them in order to find what requirements they set on the software development process itself. The aim is to evaluate the effects of EU legislation on the entire *Software development lifecycle* (SDLC) and present recommendations on what changes need to be done and what organisational structures need to be in place to make sure, that these changes are done effectively. Lastly, this thesis aims to provide recommendations to Company X on what they need to do in order to be compliant with the current effective regulations and how to be prepared against near future EU regulations. The research questions of this thesis are:

RQ1: What changes do the recent EU regulations cause to Software Development methods?

RQ2: How are the necessary changes accomplished?

The research questions help this thesis to tackle the research problem in a two-folded manner. RQ1 is used to find out what actual new requirements the recent EU regulations put on the software developers. After finding the required changes the logical next question would be, how are these changes accomplished. RQ2 is used to represent that line of thought, both on what measures and protocols need to be implemented to who is responsible and overseeing these changes.

1.3 Research methods

This thesis uses a literary review to explain the background topics related of Software development and EU regulations. Google Scholar was the main tool used to find and select applicable sources discussing the SDLC. The EU regulations were used as primary sources for finding the new requirements that cause changes to software

development methodologies. The selected literary sources were used to lay out the basic theory of the selected topics and lay down the basic principles that the thesis will follow.

The review and presentation of software development was focused on the different development models and the different work phases of SDLC. The used sources were mainly primary sources from the original inventors and authors of development models, or from materials used to teach the principles of these models or the different purposes of the phases in SDLC. The sources regarding the different EU regulations were from the archives of EU, as this thesis focuses on the requirements from the different regulations themselves.

The other data collection method in this thesis was a set of interviews at Company X to refine the requirements found using the literary review. A qualitative analysis is then performed on the interviews to finalise the list of requirements and the list of recommended actions overall and more specifically to Company X.

1.4 Thesis structure

In Chapter 2, the different phases of SDLC will be explained. After them, a selection of widely used development models are also discussed. The models are examined through the lens of workflow between the different SDLC phases that they all have in them in one form or another.

Chapter 3 examines the current trends of EU on what type of regulations they aim to put into effect. The broader EU strategy in terms of digitalisation and the adaption of new technologies is discussed. Slightly older but still impactful EU regulations of GDPR and *Digital Operational Resilience Act* (DORA) [5] are introduced, and their contents are laid out. GDPR is also used to find some requirements that have already been adapted by software developers.

The AI Act is introduced in Chapter 4. The AI Act will be the main piece of

regulation that will be analysed for requirements, and for that reason the AI Act is combed through thoroughly to explain its contents in Sections 4.1 and 4.2. The requirements that have been found based on the literary review are presented in Section 4.3.

Chapter 5 is for the interviews. The questions of the interviews are presented, and the interview results are analysed. Chapter 6 summarises this thesis and discusses the results. After the discussion, the Research Questions are answered. Also in Chapter 6, the shortcomings of this thesis are discussed and some additional research on this topic is recommended.

2 Software Development

Software development is a complex endeavour which requires much more than just programming. It includes activities like requirement analysis, design and testing. In short, the goal of software development is to design and implement a solution for a user that has provided the specifications on what they need. The term *software development* is not to be confused with the term *software engineering*. Software development is a part of software engineering, which also encompasses additional aspects that are not part of software development, like organizational and project management.

Software development is typically conducted using different development methodologies or models. Older models like the Waterfall model are more linear in nature, as in Waterfall model a phase must be fully completed before moving to the next step [6], and later ones like Agile models have more iterative elements in them. [7] All models have different strengths and weaknesses in them, and these characteristics need to be considered, when choosing the model for a software project. All these models however contain similar distinct phases in their development cycles.

This chapter will present the different phases of a *software development lifecycle* (SDLC) and discuss the different tasks that are within each phase. After that, Section 2.2 presents some of the most widely known and used software development models and explains, how the different phases are utilised in the models.

2.1 Software development lifecycle

Software development lifecycle or SDLC is a term that refers to a general framework for the different phases of software development. [8] The development process starts with a feasibility estimation. Assuming that the software is deemed financially feasible, the development process moves to analyse the problem it aims to solve and to the designing phase of the software itself. After that, the programming gets underway, the program is tested along the way and when it is finished it will be launched into production. For this thesis, six individual phases will be presented each with their own sections.

2.1.1 Feasibility

Feasibility analysis is the first phase of SDLC, where the ideas for a piece of software are examined in order to determine, will that piece of software be developed. These ideas for a software product can come from anywhere. They can be from customer suggestions, market research, internal software development staff among other sources. [9]

Typically, the ideas are first analysed through the lens of economic feasibility by the marketing department. *Economic feasibility* means in this context things like how the planned product fits into existing channels of distribution, does the planned product affect existing product lines and does the planned software fit with the company´s planned market objectives. [9] Basically, the idea is evaluated to make sure that the software project makes business sense. [10] Typically the return-on-investment (ROI) is integrated into this phase, meaning mathematical estimations on does the project provide the necessary monetary returns to the business. [10]

The Feasibility phase is not just financial analysis, as there might be other non-monetary benefits that the software project may provide to the company. Usually, a document is created that states the needs that the software would solve [9] and

what is called a high-level forecast or budget, that gives a high and a low estimate on the budget and timetable for the software project. [10] The decision to continue the development process is made from the information provided by these documents.

2.1.2 Analysis

After the software project has been deemed feasible in business sense, the *Analysis* phase of SDLC will commence. This phase starts typically with a *requirements analysis*, where the end result is a document which outlines all of the technical specifications for the programmers so that they do not need to go back to the users directly for clarification. [10] This process can be difficult as there are multiple things that can hamper the process of defining the requirements for the software. The users can have different needs from each other that can even be incompatible with each other. They might even change their needs during the development process. [10]

This process of analysing the needs of the future users of the software is iterative in nature and it requires the people who are planning the system to decompose the system into smaller components that each have a defined function that helps the software to achieve its goal. [10] Different types of charts like data-flow diagrams and entity relationship diagrams are used to present the underlying logic of the system. [10]

Functional requirements are not the only things that need to be considered in this stage. Other aspects like how well it must perform its task or for how long will this system be in use are also requirements that need to be analysed for the system to be well suited to the needs of its future users.

2.1.3 Design

Design phase will commence after the requirements have been analysed and decided. The requirements will be used to make decision on the actual production of the

software, like what programming languages will be used or what platforms will the program be run on. [10] Design is basically the process where the software system is conceptualised before it will be implemented. [11]

Unlike the analysis phase, the design phase requires less of a mathematical and engineering focus as the the design process is much more creative endeavour where the creativity, past experience and a sense of what makes "good" software are key success factors. [10] Basic design principles also help the designers to reach better end results. These basic design principles are things like recognising if the design process suffers from tunnel vision; not inventing the wheel again or the design should be structured to accommodate change. [12]

The process of designing software also includes the creation of different models for the software system. The models are used to picture different aspects of the software, its components, their functions and relations to each other. Prototypes of different components of the software can also be created in this phase. It is much rarer to develop a prototype of the entire system, as it usually is unnecessary. Prototyping focuses on functionalities which are not certain to be technically successful. [9]

2.1.4 Programming

Programming is the phase of SDLC where the actual software is built. This phase can be either iterative or linear in nature depending, what development model is being used. During this phase the requirements might change, or some problems can arise that apply pressure to change the requirements of the system. Modern programming uses quality requirements like *reliability*, *robustness*, *usability*, *portability*, *maintainability*, and *efficiency* to measure the performance and quality of the software. [13]

Programming is done by programmers, who use a variety of tools to assist the programming process. The main tool is typically an *integrated development envi-*

ronment (IDE), which is a program that contains tools like a source-code editor, build automation tools, and a debugger. The actual programming work is done via an IDE and that includes tasks like writing, modifying, compiling, deploying and debugging software.

Programmers have developed best practises and conventions to prevent avoidable mistakes and errors, as most of written code will not be maintained by the same person throughout its lifecycle. Maintainability measures how easily a piece of software can be maintained, and it is an important metric, as 40%–80% of the lifetime cost of a piece of software goes to maintenance. [14] These best practises and conventions also help avoid undesirable patterns forming in the code like coupling. Coupling means that programs are reliant on each other. This means that one change in a program forces changes to be made also in other parts of the program. [10]

Programming requires documentation to be written of the code, and it should explain how the software operates or how it can be used. This documentation can be within the source code, or it can be in external documents. Documentation can be aimed at other developers or for the users and that affects what it contains. Documentation also helps increase maintainability.

2.1.5 Testing

The goal of testing is to make sure that the software runs correctly and without errors. Software testing helps the developers to gather information about the software, like how good is the quality of the software and what is the risk of its failure. [15] It has to be noted that for software that has even the tiniest bits of complexity in it, it becomes impossible to *fully* test it, either for all the different inputs or for all possible states of the software. [16] Testing can be used to see if the software works correctly in some defined scenarios but it cannot be used to determine if it works in all scenarios.

Testing happens in multiple different spots in the development cycle and by different people. Once a developer has written a piece of code that performs a complete function or sub-function, the developer should do debugging for that code. In *debugging*, developers make sure that their code in a program works as designed. [10] Debugging will occur concurrently with the developing process in the Programming phase.

Before new code is committed to the overall software project, the code should go through a *code review*, where a group of people evaluate the new code for possible quality problems. Additional benefits to this are improved code quality, increased likelihood finding better solutions, and knowledge transfer among others. [17]

Quality assurance tests the entire software product for its accuracy. Larger organisations have an entire separate organisation for Quality assurance and their sole task is to conduct the quality assurance process. Typically, this is accomplished with *acceptance tests*. [10] Acceptance tests are generated from the original software requirements and for that reason an acceptance testing plan is designed and implemented during the Analysis and Design phases, but the acceptance tests are conducted during the Testing phase. [10]

2.1.6 Production

The production phase comprises the tasks of providing the software to the customer and the maintenance of the product after its release. The specific tasks that need to be performed, are dependent on the type and complexity of the software. The production phase is not normally an event that is done only once for each piece of software, as all the possible updates and other improvements also need to be distributed to all instances of the software. For some systems the upgrades can happen quite often and that requires the development and usage of efficient and sophisticated deployment pipelines.

The deployment of a system or software consists of different types of activities, some of which are not related to software development at all. The general types of activities are *stakeholder communication*, *installation preparations*, *installation*, and *testing the installed product.* [18] As these are general activity types, not all of these are applied in every single software production phase. More complex deployments include other additional activities, and simpler deployments might not require all of the general activities.

The production phase does not end with the successful deployment of a system or an update. Software maintenance has been understood to mean the work that is done on the software after it has been put into use. [19] This work is comprised of tasks like correction of errors, and the improvement, deletion or addition of functionalities. [19]

Maintenance begins after the first deployment of the system, and it continues until the system is taken down. The different tasks and activities of maintenance are similar to the ones that are in other phases of SDLC, and maintenance can be considered a miniature collection of all the other phases.

2.2 Development models

Developing software with the phases of SDLC requires that the development process is structured and systematic. That requires the use of *development models*, as the phases require different things from different people depending on the phase. The phases also are not all like each other, they might have different lengths or they can be different in how sequential or iterative they are in nature.

Some of the most used and well-known development models will be presented next in order to better understand how these development phases work in the big picture. The order of presentation will go from more traditional and sequential models to more recent and iterative models.

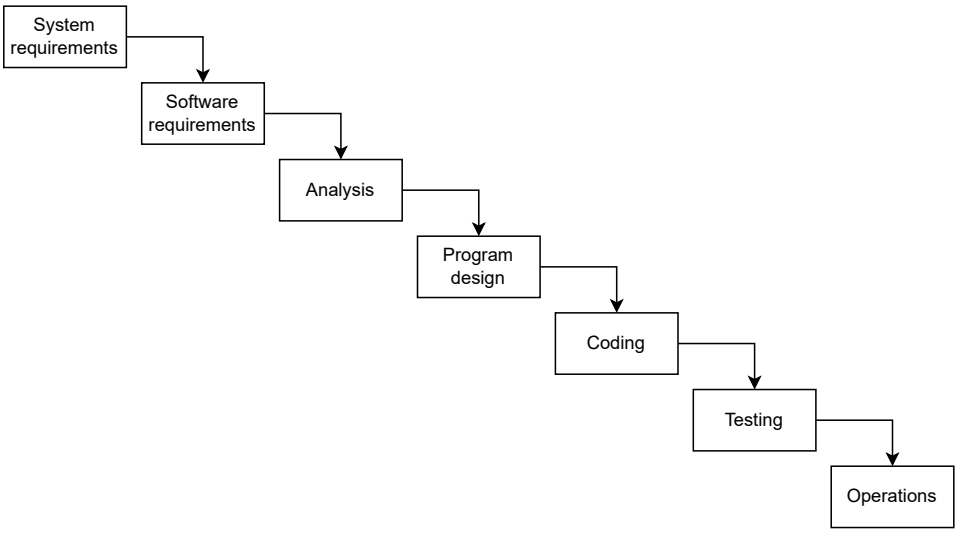

Figure 2.1: Development steps of the Waterfall model

2.2.1 Waterfall model

The waterfall model is one of the most mature development models still in wide use. First mentions of the term waterfall were in the Winston Royce´s article *Managing the development of large software systems* in 1970, where Royce presents the seven different steps needed to minimise the development risk. [20] The different steps are presented in Figure 2.1.

The waterfall model is a sequential model where each step´s results are analysed and reviewed at the end of that step. One step must be fully completed and approved before the project can move into the next step. [6] Although this model is very rigid, it is still in wide use, as Vijayasarathy et al. found out in their research, that waterfall model was used in 32% of software projects, which was the single most used development model. [21] Especially companies that have larger amounts of employees like to use the waterfall model due to its structured nature and its emphasis on comprehensive documentation.

Waterfall-based models also are thought to have more predictability on the budgeting of the project, which can be a key factor for larger enterprises. In the survey

by Vijayasarathy et al. the more traditional and larger companies that consider a higher number of their projects to be critical tended to use more waterfall-based development models. [21]

The problems that waterfall models have been criticised on deal with the fact that the model incentivises organisations to plan extensively at the start of the project, making changes more difficult to execute later in the project. This, combined with the linear nature of the model, makes the model bad at adapting and responding to a changing environment. Any changes to environment and requirements need to be re-validated and will cause previous work to become wasted. Royce himself described that only testing the software at the end during the testing step and not beforehand is very risky and it invites failure. [20] Other issues commonly found in waterfall-based models are high resource requirements for comprehensively writing documentation during each development phase, lack of user feedback, and having to carry problems from already finished phases to the following phases. [6]

2.2.2 Spiral model

The spiral model is a modified waterfall model that focuses more on risk management. The spiral model was first described by Barry Boehm in 1986 [22] and he describes the spiral model to be a more of a *"process model generator"*. In the spiral model, the project´s risks are considered carefully and from those considerations, an appropriate process model is selected for the project. [23]

The spiral model differs from other models because of its cyclic approach to development process. The accuracy or degree of definition and implementation of the system increases with each cycle, while the degree of risk decreases. The spiral model is also unique due to its use of anchor point milestones, that are designed to ensure stakeholder commitment to feasible and mutually satisfactory system solutions. [23]

The inventors of the spiral model recognised six characteristics that they will

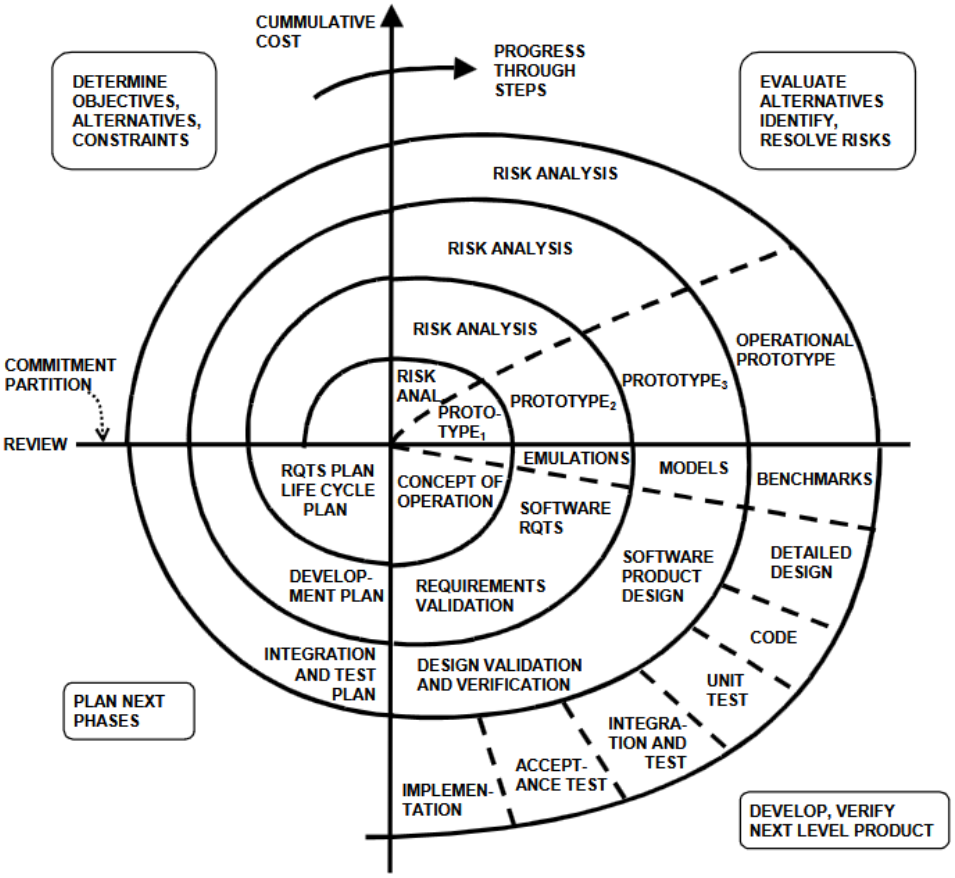

Figure 2.2: Development stages of the Spiral model [23]

adhere to, if the model is followed as intended. The first characteristic is the concurrent determination of key artifacts. Key artifacts are things like the operational concept, the system and software requirements, and the system and software architecture and design. [23] The second characteristic is that every single cycle in the model has defined objectives, constraints, alternatives, and risks that have been mapped to each quadrant of the model. These have to be completed before moving to the next cycle.

The third characteristic is that the required effort for each activity is determined by the amount of risk in it. The fourth characteristic is very similar, as it says that the level of detail is determined by the amount of risk. Anchor point milestones are the fifth characteristic and they were added to the list as a remedy to the original spiral models´ faults. [23] The sixth and final characteristic is emphasis on system and life cycle activities and artifacts. The aim of this characteristic is to avoid the pitfall of focusing only on the software construction aspects. Overall system and life cycle concerns also need to be taken into account. [23]

2.2.3 V-model

V-model is also a linear model like the waterfall model as in both of them, one work phase must be completed before the next one can begin. Where V-model differs from the waterfall model, is the early emphasis on testing. The testing procedures are developed early in the development cycle before any coding is done, more specifically during each of the phases before the implementation phase. [24]

The model gets its name from the shape that the model is presented in. The different phases fallow each other sequentially, but each of the phases after the implementation phase is bent upwards in the model to highlight the connections between the testing and development phases as can be seen from Figure 2.3. The horizontal axis represents time or project completeness, and the vertical axis represents level

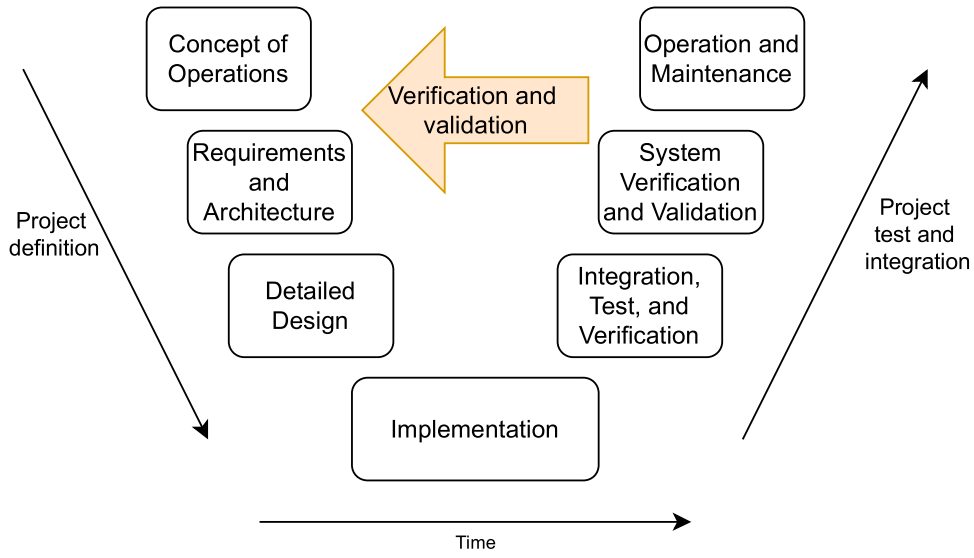

Figure 2.3: Development stages of the V-model

of abstraction.

The start point of the model is on the top-left corner, and then the steps are followed down and to the right, until the implementation step has been reached. During these left-hand side phases, the requirements of the system, the system itself and its architecture are designed. Alongside those, both the high and low-level testing plans are formed. The coding process happens in the implementation phase and then the previously formed testing plans are put to use. [24]

Advantages of the V-model are considered to be the ease of use and the clarity of what specific deliverables each phase has. The V-model has a greater chance of success over the waterfall model because of the early focus to develop test plans during the development life cycle. Some noticed disadvantages are the rigidity of the model and the difficulties to adjust the scope of the project. Software is developed only during the implementation phase and not before it, so there are no early prototypes of the software. Although the V-model does emphasise the creation of testing plans early it does not provide a clear path for problems found during testing phases. [24]

2.2.4 Agile models

The current trendy software development models and methodologies are mainly based on the ideas presented in the *Manifesto for Agile software development* from 2001. The manifesto was written by a group of 17 software developers as a result of a gathering to discuss lightweight development methods. [25] Agile methodologies focus on the collaboration between people and the adaption to a changing environment. In Agile models, the end used also has a a more integral role throughout the development process than in other more traditional models like waterfall.

The four core values of the Agile model are (1) Individuals and interactions over processes and tools; (2) Working software over comprehensive documentation; (3) Customer collaboration over contract negotiation and (4) Responding to change over following a plan. [25] These values reflect the ideas of Agile, that the goal of any software project is the creation of the software in question. Tools and documentations are useful for that, but they should not be used just for the sake of using them. It is more important to have competent people working together effectively and to be able to react to changes, than to create highly detailed documentation and requirements for the system. [26]

Most of the different development models under the Agile umbrella slice development work into small increments that minimise the amount of planning and design before the actual implementation. These iterations are short time frames lasting typically from one to four weeks. [27] During each iteration, a team goes through all the different steps or functions that are a part of an iteration. These steps are planning, analysis, design, coding, unit testing, and acceptance testing. At the end of each iteration all the stakeholders are summoned to a meeting, where the state of the software is presented to them. The basic goal for each iteration is to have a available release at the end of each iteration. [28]

Some of the most recognisable Agile models are *Scrum*, *Kanban* and *Extreme*

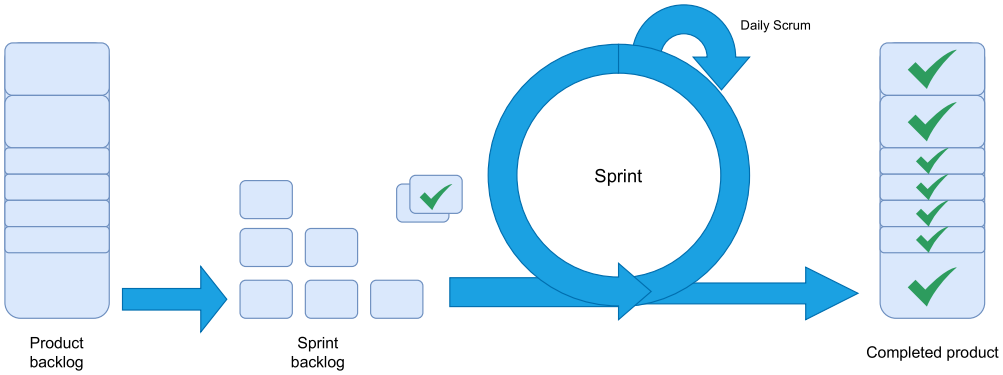

Figure 2.4: Workflow in Scrum

programming (XP), that each focus on slightly different aspects of Agile. Scrum and Kanban are more interested in managing the flow of work and XP focuses more on the development practises. All of them however share the commonalities of being more adaptive than predictive and placing the emphasis on working code rather than comprehensive documentation.

As an example, in Scrum, the development team breaks down the work into smaller pieces that can be accomplished in a single iteration, called a *sprint*. These sprints last usually two weeks, but they can range from one to four weeks. These pieces are ordered by the urgency of the task and for each sprint a selection of these work pieces are chosen to be completed in that sprint. [29] This process is illustrated in Figure 2.4.

Each day during a sprint starts with a short 15-minute meeting called the *daily scrum*, where the assignments of the day are decided. At the end of the sprint a *sprint review* and a *sprint retrospective* are held. These are used to evaluate the success of the sprint and determine what can be improved in the development process. [30]

3 Current landscape of EU regulations

For a long time, the product standards of ICT industry have been developed by international informal bodies. This has created problems that national consumer protection laws created by national formal bodies are not quite enough to handle. [31] The need for legislation that protects users whilst also not stifling innovation and development of the developers is great but achieving that delicate balance has been a difficult and daunting task for legislators so far. [32]

Different EU institutions have been looking for ways to harmonise regulations between different member states and in the field of ICT, the current method for harmonisation has been the usage of EU regulation. [33] Directives have been previously one of the larger methods to create harmonisation and standardisation between the different EU member states, but the usage of directives caused some issues when they were applied into binding law. Directives are not binding in themselves, meaning each member state can implement the directive differently from each other. [34, Article 288] Directives can cause uncertainty by incorrect or non-implementation of a directive. [33]

EU´s use of regulations over directives in certain fields helps lessen the legal uncertainty and a fragmented patchwork of laws from different member states. [33] The regulations that EU typically legislates are directly effective and they do not

need other additional implementation from member states. [33]

In this chapter, the current landscape of European Union´s regulation regarding software development is introduced. The EU *Digital Decade* program is introduced, and the general intentions of EU are discussed. After that, the *GDPR* is introduced and analysed for the requirements it has for software development. These requirements are categorised into two categories, and they will be used later in this thesis as the baseline for what kind of changes new legislation packages from the EU cause. After *GDPR* the *DORA* legislation is introduced. DORA will be analysed later in order for to find out how these new requirements are implemented and made sure that they are understood and followed correctly.

3.1 Digital Decade

In 2022 European Union launched the *Digital Decade Policy Programme 2030* as a means to create a transparent plan for the citizens and companies to see and adapt to. [1] The Digital Decade Programme has stated objectives like the creation of a

> *"digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values" and promotion of "a Union digital regulatory environment to support the ability of Union undertakings, especially that of SMEs, to compete fairly along global value chains". [1]*

Alongside the objectives, the policy program sets out numerical targets that EU aims to meet during this program. These targets are for example, at least 75 % of Union enterprises have taken up at least one of the following technologies: cloud computing services, big data or artificial intelligence. [1, Article 4] The Digital Decade Programme also sets out the groundwork for facilitating *multi-country projects* that will help achieving the goals set out in the program. [1, Article 4]

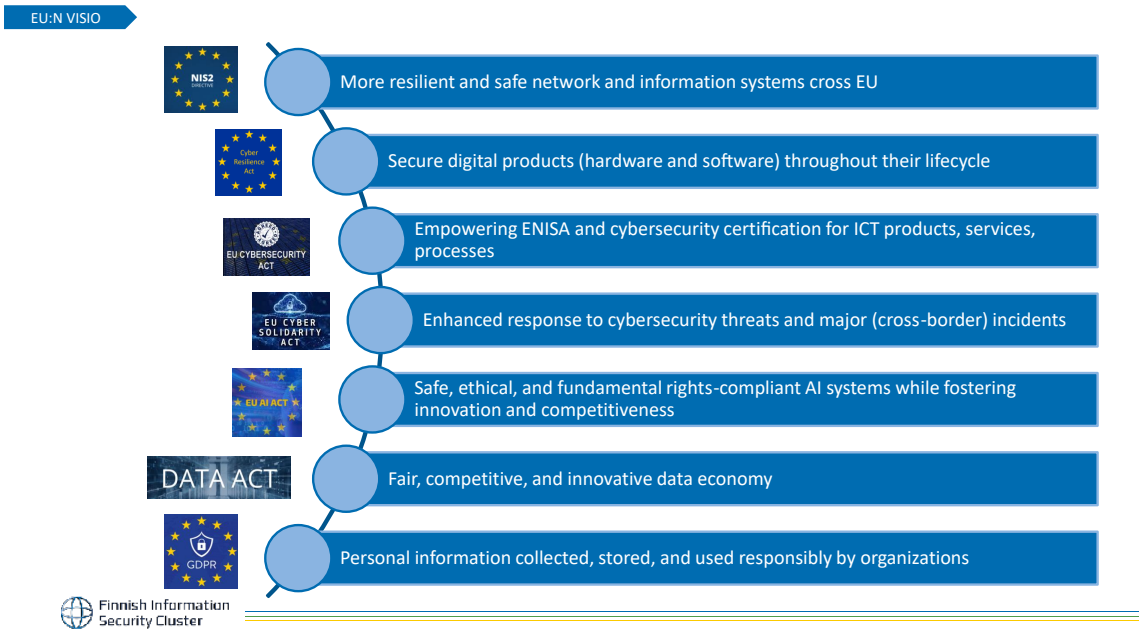

Figure 3.1: Vision of the EU legislation [35]

With this Digital decade program, EU has already either passed or drafted multiple legislation packages handling different aspects of digital infrastructure. This is a culmination of a longer trend of EU inserting legislation targeting aspects that have previously been handled in the industry as codes of good conduct and informal quality standards. Figure 3.1 shows some legislation packages that EU has drafted or passed in the last 10 years and what their general goal and idea is. The legislative packages mostly deal with *cybersecurity* and *data protection*, but the general principle can be inferred from them and applied to other legislative aspects of the Digital Decade.

EU has used the term *codes of conduct* in legislation since the 1990s, but the meaning was not clear, as its use was quite fragmented and the label of "code of conduct" was given to a wide array of different legislative tools. [4] Researchers have identified five categories for the codes. These categories do not have absolute determining factors due to the nature of the lack of framework for the usage of the

term codes of conduct. The determining factors are roughly, who are the actors that the code targets. [4] The paper by Carl Vander Maelen lists five groups for these codes but mentions, that the pinpoint identification for the group is extremely difficult because the lawmakers also had been referring to codes inconsistently. [4] The different groups are defined by the group that the code aims to affect. Group 1 codes deal with EU institutions and Group 3 handles the direct interactions between EU institutions and private sector actors. [4]

In more recent times from around 2018 onward EU has adopted a new direction for the usage of codes of conduct. The new codes of conduct used in legislation like *GDPR*, *Audiovisual Media Services Directive* (AVMSD) and *Digital Services Act* (DSA) appear to be harder than previous iterations of the usage of codes. This appears to be in line with the broader ongoing pattern where EU has interconnected hard and soft norms in legislation more than before and in increasing numbers. [4] The EU naturally nudges its legislative tools to the harder side in time due to the integrative dynamics that drive the EU. [36] GDPR mentions, that codes of conduct are instruments intended to contribute to the proper application of the GDPR. [2] This newer style of hard codes of conduct has the goal to include aspects of software development, that were previously considered to be informal good practises, in the EU law itself.

3.2 General Data Protection Regulation

General Data Protection Regulation (GDPR) is an EU regulation dealing with the "protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data". [2, Chapter 1, Article 1] As GDPR is an EU regulation and not an EU directive, it is legally binding in its entirety and so the EU member states do not need to create their own regulations on this subject matter. [2, Chapter 11, Article 99] The regulation came into force

on 25 May 2018.

As GDPR has been in effect for a few years now, its effects have become more known globally and it has been an influence on many different data protection legislations from other parts of the world. [37][38] The impact of GDPR is from both the actual legislation itself and also from the awareness from general population on the topic of data protection. [39]

GDPR applies to the processing of personal data wholly or partly by automated means. GDPR also applies to other un-automated means of processing personal data which form or are intended to form part of a filing system. [2, Chapter 1, Article 2] The same article does also include exceptions, when GDPR does not apply. The territorial scope, as the legislation itself puts it, of GDPR does apply to all data controllers or processors that handle personal data of EU citizens regardless where the actual processing is being done. [2, Chapter 1, Article 3]

3.2.1 Requirements from the articles

The articles of GDPR are analysed here for the relevant parts regarding software development. The analysis produces *Product Requirements* that are abbreviated **PR** in this thesis. GDPR mainly handles the matters of personal data protection and rights and responsibilities of data subjects and data controllers.

Articles 12 and 13 discuss the information that the data controller has to provide to the data subject when the personal data has been collected. This data includes for example the following things: the purposes of the processing of the personal data, the recipients or categories of recipients of the personal data, the period for which the personal data will be stored and the existence of automated decision-making, including profiling. [2, Chapter 3, Article 13] (**GDPR.PR1:** The data controller must provide certain required information to the data subject when requested).

Article 30 also discusses the same subject matter from the perspective of the

data controller. It says that the data controller must keep a record of the processing activities under its responsibility. The record has to include for example the following information: the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; where possible, the envisaged time limits for erasure of the different categories of data; among other data mentioned in the previous paragraph. [2, Chapter 4, Article 30] (**GDPR.PR2:** The data controller must keep a record of processing activities)

In cases, where the data subject notices that their data is incomplete or incorrect the data subject has rights that they can exercise to correct or remove the incorrect or incomplete data. Articles 16 and 17 lay out these rights and more specifically article 16 tackles the rectification of incorrect data and completion of incomplete data. [2, Chapter 3, Article 16] Article 17 lists the cases when data subject can demand the data controller to remove the data. [2, Chapter 3, Article 17] (**GDPR.PR3:** Personal data must be either corrected or deleted when requested in applicable situations)

The data subject can also request that the processing of personal data is restricted in certain conditions like, that the data subject contests the accuracy of the personal data or that the processing is unlawful, but the data subject still opposes the deletion of their personal data. In cases like these all processing (with the exception of storing the data) has to have data subject´s consent or it has to be for the legal protection of another individual's rights or for the important public interest of the European Union or a member state of the EU. [2, Chapter 3, Article 18] (**GDPR.PR4:** Personal data must be able to be left outside of processing when needed)

The data subject has the right to object to the processing of their data and to automated decision-making, which also includes profiling. The controller must stop the processing, when they have received this objection and they can only continue the

processing when they have presented the data subject with "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject". [2, Chapter 3, Article 21] Automated decision making is something that the data subject can opt out of in certain situations where the decisions would have legal or other similar effects on the data subject. [2, Chapter 3, Article 22] (**GDPR.PR5:** Data processing can have automated decision-making in it, but it has to be able to be removed from certain sets of data)

3.2.2 Synthesised requirements from GDPR

Although the articles of this piece of legislation are mainly concerned on the processing of personal data, technical requirements for software development can be inferred from them. In this sub-chapter the synthesized *Development Requirements* will be presented and they will be abbreviated as **DR**.

GDPR.PR1 and **GDPR.PR2** discuss the matters of the personal data and metadata, that the data processor possesses. These requirements can be achieved by introducing developmental requirements in the software development organization that make sure that in every system that uses personal data this is made a priority already in the design phase. In the developmental organization, there should either be a person that is responsible for making sure that these are included in everywhere where it is necessary, or a check for this is introduced in pull request processes. (**GDPR.DR1:** The development has to include a method to make sure, that all data handling processes in the developed program are logged and saved for possible lawful requests by data subjects)

Chapter 4 of GDPR describes the obligations of the data controller and processor. In article 24, the general obligations of the controller are listed, and they include obligations like, the implementation of appropriate technical and organisational measures to process personal data in accordance with GDPR. The same

article also stipulates the data controller to adopt appropriate data protection policies, when they are not disproportionate in relation to the data processing activities. [2, Chapter 4, Article 24]

GDPR.PR3 and **GDPR.PR4** also mandate that the collected data has to be corrected or deleted when requested and when needed, personal data must be left outside of processing. These *Product Requirements* also give hints on what the development process itself should look like alongside Article 24. They all deal with how the data processing should be changeable, trackable and possibly even withheld from the processing. Similarly same critical view and possibility to make changes should be adopted on the entire software development process. (**GDPR.DR2:** The software development organisation has to have mechanism within it that review and change the development methods when they are detected not to be in accordance with regulations)

Article 25 describes the principle of "Data protection by design and by default", where data controller needs to implement appropriate measures (both technical and organizational) to ensure that data-protection principles that have been mandated by GDPR have been fulfilled. The same article also discusses the obligations to limit everything about the collection and processing of personal data to only that what is necessary for each specific purpose. [2, Chapter 4, Article 25] (**GDPR.DR3:** The used development methods must be adapted to have data protection by design in it from the start)

Article 32 describes the different measures the data controller has to be able to do to ensure that data processing is secure. These measures include pseudonymisation and encryption of data; the ability to restore access to personal data in a timely manner after an incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing among other things. [2, Chapter 4, Article 32] **GDPR.PR5** also shows

this idea with the aspect of automated decision-making, but with the caveat that all these new technologies must be evaluated on where they can be applied for the application to be GDPR compliant. (**GDPR.DR4:** When developing software to be used in data processing, the used techniques and technologies should be as state-of-the-art as is appropriate considering the scope and nature of the data processing)

GDPR also describes different interactions that data controllers and processors should have with supervisory authorities. These interactions include things like notifying the authorities within a 72-hour time period of personal data breaches [2, Chapter 4, Article 33], or cooperating with authorities when requested by those authorities. [2, Chapter 4, Article 31] (**GDPR.DR5:** The development organization should have a structure within it that makes sure, that request from authorities are acted upon)

In situations, where the data processing would cause a high risk to the rights of the data subject, the data controller has to conduct a Data protection impact assessment before processing personal data. These assessments should at least assess that the purpose of the processing is necessary and proportional. They should also describe the planned processing operations alongside with the reasons why the controller needs to do those operations. The assessment should also have descriptions on planned methods to mitigate the risks caused by the planned processing. [2, Chapter 4, Article 35] (**GDPR.DR6:** During development data use cases should be considered early so that the risks can be recognised, and those risks could be addressed)

3.3 Digital Operational Resilience Act

Digital Operational Resilience Act or DORA is an EU regulation that aims at strengthening the IT security of financial entities such as banks and insurance companies. It entered into force on the 16th of January 2023, and it has been applied

from January 17th 2025 onwards. [40] The core themes that this regulation handles are IT risk management and preparations and measures for operational disruptions.

The modern world relies heavily on IT in every aspect of society. It has made it possible to create complex and interconnected systems. This reliance on digitalisation and interconnectedness of IT has also increased and amplified the risks, making society and especially financial institutions more vulnerable to cyber threats or ICT disruptions. [5, Recital 1] The regulation describes its task in the following way

> *This Regulation aims to consolidate and upgrade ICT risk requirements as part of the operational risk requirements that have, up to this point, been addressed separately in various Union legal acts. [5, Recital 12]*

The most important term used in DORA is *digital operational resilience*, which means the ability of a financial entity to build, assure and review its operational integrity and reliability. They can handle these issues themselves directly or they can use a third-party service provider for that, as long as the ICT-capabilities that are required for the continuous provision of financial services are supported even throughout disruptions. [5, Article 3, Paragraph 1]

Chapter 2 of DORA lays out the requirements for ICT risk management. It mandates financial actors to create and maintain an *ICT risk management framework* as part of their overall risk management system. The framework must include at least strategies, policies, procedures, ICT protocols and tools that are necessary to protect all ICT and information assets. [5, Article 6]

Financial entities are also mandated to map out all different business functions and roles that are supported by ICT and identify all sources of ICT risks. [5, Article 8] These identified tools and risks are then used by the financial entities to continuously monitor and control the security and functioning of their systems [5, Article 9] and be on alert for any anomalous activity. [5, Article 10] Part of the ICT risk management framework is the creation and upkeep of an *ICT business continuity*

policy, which includes mechanisms and plans for continuing business operations in case of ICT related incidents. [5, Article 11]

Chapter 3 of DORA handles regulation regarding ICT-related incident management. Financial entities are mandated to establish a process with the goal to detect, manage and notify ICT-related incidents. All ICT-related incidents and cyber threats need to be recorded and the root causes for these incidents need to be identified in order to prevent future occurrences of such incidents. [5, Article 17]

These incidents and threats are to be classified, and their impact is to be determined by the financial actors. [5, Article 18] Major ICT-related incidents have to be reported to relevant authorities and also to the customers of these financial entities, if the financial interests of these clients are affected. Financial actors can also report significant cyber threats to relevant authorities, but that is on a voluntary basis. [5, Article 19]

In Chapter 4 of DORA, the requirements for the creation of *digital operational resilience testing program* are laid out. The purpose of this testing program is the identification of weaknesses and gaps in digital operational resilience. The testing has to be done by an independent team, but it can be internal or external. [5, Article 24] ICT tools and systems that financial entities use must be tested with appropriate testing measures. [5, Article 25]

Financial entities must conduct a *threat-led penetration test* (TLPT) every 3 years. [5, Article 26] TLPT is a testing technique where a team tries to disrupt or otherwise cause harm using real-life techniques and tactics to the financial entity´s systems. [5, Article 3, Paragraph 17] The article places limitations on who are allowed to conduct the testing, as they need to provide proof of competence and expertise on the subject matter of threat intelligence, penetration testing and red team testing. [5, Article 27]

Financial entities also need to manage risks of third-party service providers that

they have contracted. This means, that financial entities have to have a strategy that they regularly review on ICT third-party risk. [5, Article 28] The strategy contains at least the scenarios of acquiring a new third-party ICT service provider; evaluating current third-party providers; and exiting the contacts of current third-party providers. [5, Article 28]

Financial entities are also allowed to share cyber threat information and intelligence if the information sharing aims to enhance the digital operational resilience of financial entities and the entities are within communities of trusted entities. [5, Article 45]

4 Artificial Intelligence Act

Artificial Intelligence (AI) Act is a brand-new legislation from the European Union. It has been adopted and put into force on August 1st, 2024. As a part of EU´s digital strategy, the European Parliament wants to regulate AI to make sure that the development and use of AI technologies have a good environment and that they would pose as minimal of a risk as possible to the users. [41]

The aim of the AI Act is to create the foundation of legal framework for the development and use of AI in the EU. [3] European Parliament has recognised the future benefits of AI technologies and the fact that some member states of EU have started to explore the adoption of national rules for AI. Differences between each member states´ legislation can cause fragmentation of the internal market of the EU and that can cause lower legal certainty for companies and other operators that use and develop AI technologies. [3]

One of the goals of the European Parliament is to

> *"achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market should be prevented by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market" [3]*

The AI Act fulfils these aims by creating a harmonised ruleset for AI systems;

prohibiting certain AI practises; creating risk-levels for different types of AI and generating different requirements for these risk categories; creating rules for transparency and generating measures to support innovation in the field of AI in the EU. [3, Chapter 1, Article 1]

Alongside these measures, one of the goals of the AI Act was to create a "technology-neutral, uniform definition for AI that could be applied to future AI systems". [41] In the AI Act Chapter 1 Article 3, AI system is defined in the following way:

> *"AI system means 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". [3, Chapter 1, Article 3, Paragraph 1]*

4.1 Definitions

Chapter 1 of the AI Act describes the general provision of the act and in it is the Article 3 which lists the definitions for all the terms the Act uses. The first set of terms all deal with the different roles that surround AI systems. These roles include for example *provider, importer, deployer* and *operator*. A *provider* is a person or an organization that develops an AI system or a general AI model or has some other person or organization develop it for them to put it on the market. A *deployer* is a person or a public agency or other body that uses an AI system with the exception of personal non-professional use. [3, Chapter 1, Article 3, Paragraphs 3-4]

An *importer* refers to a person that brings an AI system from outside the EU and places it on the market in the EU. A *distributor* is a person other than an *importer* or a *provider* that is a part of a supply chain for an AI system to be put

into the EU market. The last introduced role in the Act is the *operator* which is an umbrella term that can refer to a provider, product manufacturer, deployer, authorised representative, importer or distributor. [3, Chapter 1, Article 3, Paragraphs 6-8]

These terms for different roles include phrases like "placing on the market; making available on the market" and "putting into service". These phrases all refer to the action of bringing or supplying an AI system in the EU market. Other defined phrases that deal with the actions of *providers* and other roles in the supply chain of AI systems are "recall of an AI system" and "withdrawal of an AI system". The recall version means any action to return the AI system to the *provider* or disabling the use of an AI system made available to *deployers*. The withdrawal of an AI system refers to any and all methods that aim to prevent an AI system in the supply chain being made available on the market. [3, Chapter 1, Article 3, Paragraphs 9-11]

The AI Act also includes mentions of different types and uses of data in AI systems. Data that is being used to train the AI system´s learnable parameters is naturally referred as *training data*. *Validation data* is used to evaluate and tune the performance of the trained AI system and its non-learnable variables. When the AI system put into the EU market, it has already been tested using *testing data* to confirm the expected performance. Of course, when the AI system is in use, it will be given some *input data* which the system uses to produce an output. [3, Chapter 1, Article 3, Paragraphs 29-33]

The AI Act created the general definition for an AI system and alongside it also has listed some definitions for certain types of systems for some specific purposes. The common factor for these separately mentioned system types is their use of *biometric data*. Biometric data means personal data that is based on the physical, physiological or behavioural characteristics of an individual like facial recognition. [3, Chapter 1, Article 3, Paragraph 34] These separately mentioned systems include

systems like *Emotion recognition system* that uses biometric data to identify emotions or intentions of an individual or *Biometric categorisation system* that is an AI system that takes biometric data and uses it to categorise individuals. [3, Chapter 1, Article 3, Paragraphs 39-40]

4.2 Contents of the AI Act

4.2.1 Banned practises

The AI Act lists out AI practices that are strictly prohibited by the Act due to them having an unacceptable risk of causing harm to people. [41] These banned practises include techniques like AI systems that have subliminal effects to a person or a group to change their behaviour unconsciously in a way that causes them harm. [3, Chapter 2, Article 5]

Other prohibited practices included are, for example: AI systems that find and exploit vulnerabilities due to age, disability or social or economic status and use them to change the behaviour; AI systems that evaluate persons or groups and scores them based on their behaviour or predicted behaviour and uses those scores in unrelated situations to cause unfavourable treatment; AI systems that infer emotions of a person in workplaces or in educational institutions, except when the system is used for safety or medical reasons. [3, Chapter 2, Article 5]

The same article also describes the limited situations, where law enforcement may use "real time" biometric recognition AI systems in public spaces to locate specific persons, like victims or perpetrators of a serious crimes. The article mandates, that for each singular use of the system must be approved beforehand by a local judicial authority. In some situations, where the need is justifiably urgent, the system may be used before getting the approval, but the use must be stopped, and the results and the data must be deleted if the approval is denied. [3, Chapter 2, Article 5]

4.2.2 High-risk AI systems

The AI Act also introduces the classification of a *High-risk AI system* and the regulations and obligations for those. An AI system that is high-risk means that it negatively affects safety or fundamental rights of people. [41] Article 6 mentions two different types of high-risk systems. The first type are those systems that are a part of or used in products that fall under different EU legislation like product safety.

The second type are the systems that fall in the specific categories listed in the Annex III of the AI Act. These categories are biometrics; critical infrastructure; education and vocational training; employment, workers' management and access to self-employment; access to and enjoyment of essential private services and essential public services and benefits; law enforcement; migration, asylum and border control management; and administration of justice and democratic processes. [3, Chapter 3, Article 6] This list of categories can be amended by the European Commission by adding or modifying use-cases if the necessary requirements are fulfilled. [3, Chapter 3, Article 7]

EU will also create a database for these high-risk AI systems, where the providers of those AI systems will submit the required information. [3, Chapter 8, Article 71] These data entries include things like descriptions of the system´s indented purpose and it´s operating logic. [3, Annex VIII] This database is public, and it can be easily accessed. The article also mentions that the information in the database should be easily navigable and machine-readable. [3, Chapter 8, Article 71, Paragraph 4]

Providers of high-risk AI systems also need to create a *post-market monitoring system*, which basically includes any and all means of collecting and reviewing experience gained from the use of AI systems in order to identify any need to immediately apply corrective or preventative actions. [3, Chapter 1, Article 3, Paragraph 25]

4.2.3 General-purpose AI systems

Chapter five of the AI Act discusses matters regarding to General-purpose AI. The Act defines general purpose AI in the following way:

> *"general-purpose AI model means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market". [3, Chapter 1, Article 3]*

This describes AI systems that have been in the public's eye in recent years, like OpenAI´s ChatGPT or Microsoft Copilot. The field of General-purpose AI is rapidly advancing and current estimates say that a strong impact on business sectors like health and manufacturing alongside many others. [42]

Tambiama Madiega mentions in his article addressed to the members of European Parliament that the characteristics of general-purpose AI, like size, opacity and potential to develop unexpected capabilities beyond those intended by their producers raise a lot of ethical and societal questions on the risks that these systems can pose. *Large language models* like ChatGPT and other types of general-purpose AI can be used to spread misinformation and disinformation more efficiently than before. The AI models can discriminate if trained improperly or they can give inaccurate or incorrect information. [42]

The AI Act gives special attention to general-purpose AI systems that have a *systemic risk*. systems that have systemic risk have additional obligations they have to adhere to. Systemic risk has been defined in the following way

> *"a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain". [3, Chapter 1, Article 3, Paragraph 65]*

The *high-impact capabilities* refer to capabilities that match or exceed the capabilities in the most advanced general-purpose AI models. [3, Chapter 1, Article 3, Paragraph 64]

A general-purpose AI system is considered to have a systemic risk if it is evaluated to have high-impact capabilities with appropriate tools and techniques. It can also be deemed to have a systemic risk based on a decision of the European Commission, other relevant authorities or a qualified alert from the scientific panel. A general-purpose AI is presumed to have high-impact capabilities, when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}. [3, Chapter 5, Article 51] AI Act has used the following definition for the AI regulatory sandbox

The *AI Office* that is created by the AI Act will create *Codes of practice* for providers of general-purpose AI system collaboratively with these providers and other relevant stakeholders. These Codes of practice will be designed to include details on how to fulfil the requirements of the AI Act regarding general-purpose AI systems. The Codes of practice will be ready the 2nd of May 2025 by the latest. [3, Chapter 5, Article 56]

4.2.4 Measures in support of innovation

In The AI Act EU member states promise to create at least one national level *AI regulatory sandbox* per member state. These sandboxes should be operational

by August 2nd, 2026. The article that describes the AI regulatory sandbox also gives the opportunity for member states' relevant authorities to create this sandbox jointly. [3, Chapter 6, Article 57]

> *"a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision". [3, Chapter 1, Article 3, Paragraph 55]*

The *sandbox plan* mentioned in the definition of the AI regulatory sandbox is a document that describes the "objectives, conditions, timeframe, methodology and requirements for the activities carried out within the sandbox". It is agreed between an AI system provider and a regulatory authority. [3, Chapter 1, Article 3, Paragraph 54]

The AI Act has listed five (5) objectives for the regulatory sandboxes. They have been labelled with letters from a to e. Objective *a* states that the sandbox aims to create legal certainty and help AI system providers to achieve compliance with this regulation or other possible applicable national or EU laws. Objective *b* says that the sandbox aims to help sharing best practices with the cooperation of authorities. Objective *c* is to generate innovation and competitiveness in the AI ecosystem. Objective *d* states that the sandbox tries to contribute to evidence-based regulatory learning. Objective *e* is to provide an accelerated access for the AI systems to the EU market, in particular for small and medium-sized enterprises (SMEs). [3, Chapter 6, Article 57, Paragraph 8]

High-risk AI systems can be tested in real world conditions outside the regulatory sandbox when certain conditions are met. The testing has to be explained in a *real-world testing plan*, which includes details on "the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct

of testing in real-world conditions" [3, Chapter 1, Article 3, Paragraph 53] Freely given informed consent has to be obtained from the data subjects before the testing occurs.

4.3 Requirements from the AI Act

4.3.1 Banned practises

The AI Act is clear when it comes to AI practises that are prohibited. The underlying common properties of the different banned AI practises all deal with the AI system´s ability to cause harm to individuals. This harm can take many forms; it can affect the subject's opinions and thoughts or it can be used to classify people or groups based on their aspects or behaviours. To make sure that the developed AI system does not fall under these banned or other similarly harming practises, the provider has to thoroughly analyse the potential capabilities and use cases of the AI system. (**AI.DR1:** The developer of an AI system must analyse the capabilities and use cases of the AI system throughout its development and life cycle)

4.3.2 High-risk AI systems

The first set of requirements that the high-risk AI systems must fulfil deal with *Risk Management Systems*. The article describes this *Risk Management System* (RMS), is to be a planned continuous iterative process that will be run throughout the complete lifecycle of the AI system. RMS has to also go through regular systematic reviews and updates.

The same article also list the steps that RMS has to include at minimum. The steps are the identification and analysis of all reasonable risks to health, safety or fundamental rights that the AI system might cause in its proper use and reasonable use conditions and also under reasonably foreseeable misuse. The RMS has to also

include the evaluation of other risks, based on the analysis of data from the *post-market monitoring system* and also descriptions of the appropriate risk management measures aimed to minimize or eliminate the identified risks. [3, Chapter 3, Article 8]

High-risk AI systems should be tested in order to find out the best or most appropriate risk management measures. Testing makes sure, that the AI systems performs consistently in its intended purpose while simultaneously complying with the requirements. This testing can include testing in real-world conditions. [3, Chapter 3, Article 9] (**AI.PR1:** High-risk AI systems have to include a Risk Management System)

High-risk AI systems that use data sets to train, test or validate AI models are subject to *Data Governance* and *Data Management* practises deemed appropriate for the intended purpose of the system. These practices include things like, evaluating the possible biases of the data sets and how to prevent or mitigate those; evaluating the data collection processes and the origin of data; and identifying the relevant gaps in the data that prevent compliance with the regulations. The data sets have to be "relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose." [3, Chapter 3, Article 10] The same regulations apply also to other high-risk AI systems that do not employ AI models in them, but only in regard to the testing data that they use. (**AI.PR2:** High-risk AI systems that use AI models have to have data governance and management practices)

Article 11 requires that a technical documentation must be created before the high-risk AI system is placed on the market or put into use and that documentation must be kept up-to-date. Some of the aspects that it has to include are a general description of the AI system; a detailed description of the elements of the AI system and of the process for its development; and detailed information about the monitor-

ing, functioning and control of the AI system. All the aspects are listed in the Annex IV of the AI Act. [3, Chapter 3, Article 11] (**AI.PR3:** Technical documentation must be created for high-risk AI systems, and it has to be kept up-to-date)

High-risk AI systems have to be developed in such a way, that its operations are transparent enough for the deployers to interpret the system's output and use that output correctly. Alongside these transparency requirements, the AI system will be delivered with clear instructions for appropriate use. These instructions have to include things like the AI system´s indented purpose and other characteristics and limitations of the AI system. The written instructions must also include the necessary human oversight measures and the needed hardware resources for the lifetime of the system. [3, Chapter 3, Article 13] (**AI.PR4:** The AI system must have instructions with it that include the characteristics, capabilities and limitations of performance of the high-risk AI system)

High-risk AI systems are mandated to be developed in such a way, and have such human-machine interface tools, that it can efficiently be monitored by humans throughout its lifetime. [3, Chapter 3, Article 14, Paragraph 1] This human oversight has few goals that it tries to fulfil. In particular these goals are as follows

> *"prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse". [3, Chapter 3, Article 14, Paragraph 2]*

(**AI.DR2:** High-risk AI systems have to be developed so that they can be overseen by humans efficiently throughout the period where the system is in use)

When high-risk AI systems are given to the deployer, the system has to be explained in such a way, that the persons who are overseeing the system have the capabilities to properly understand the limitations of the AI system. They need to be able to detect unexpected performance of the system that can be caused

by anomalies, dysfunctions or other matters of similar nature. They need to also be aware of the possibility or tendency to automatically rely or over-rely on the output of the system. Of course, they also need the knowledge to correctly interpret the output of the system and possibly disregard, override or stop the system. [3, Chapter 3, Article 14] (**AI.PR5:** The high-risk AI system must have appropriate human-machine interface tools so that the risks of the system can be mitigated and recognised as much as possible)

Article 15 discusses the requirements for the accuracy, robustness and cybersecurity of high-risk AI systems. The article mentions that these metrics are achieved in "an appropriate level". The article itself does not define, what is considered appropriate, but paragraph 2 of this article declares that the Commission will

> *"in cooperation with relevant stakeholders and organisations such as metrology and benchmarking authorities, encourage, as appropriate, the development of benchmarks and measurement methodologies" [3, Chapter 3, Article 15, Paragraph 2]*

These systems have to reach this appropriate level consistently throughout their lifecycle. (**AI.PR6:** AI systems must have instructions of use with them and those instructions must state the levels of accuracy of the system and the relevant accuracy metrics)

Article 15 mentions, that high-risk AI systems have to be as resilient as possible when it comes to errors, faults or other similar problems within the system or the system´s environment. The article allows high-risk AI systems to have technical redundancy solutions if those are used to increase the robustness of the system. Also, AI systems that continually learn have to be developed in a way that the risk of biased outputs do not create skewed inputs for future operations is either removed or mitigated as much as possible. [3, Chapter 3, Article 15, Paragraph 4] These high-risk AI systems must also be resilient against unauthorised external parties to alter

or disrupt the use of the system. These unauthorised attempts include things like data or model poisoning. (**AI.PR7:** High-risk AI systems must be developed in such a way, that they are as resilient and robust as possible to withstand internal faults and external cybersecurity threats)

AI Act mandates *providers* of high-risk AI systems to create a *Quality management system* or QMS. Article 17 lists 13 aspects that it has to at least cover. These aspects range from a strategy for regulatory compliance and techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system to systems and procedures for data management like for example data acquisition and data filtration. [3, Chapter 3, Article 17] The implementation of these aspects can be proportional to the provider´s organisation´s size. The QMS has to be documented in a systematic manner and provided alongside the AI system. (**AI.PR8:** High-risk AI systems must have a Quality management system)

The requirements **AI.PR6**, **AI.PR7** and **AI.PR8** all either mandate the creation and maintenance of additional systems or generate certain thresholds that the AI system must meet in order to be compliant with the regulation. These requirements help the developer of an AI system to have a blueprint of what to consider, when developing a high-risk AI system. (**AI.DR3:** Developers of a high-risk AI system have to consider quality metrics like accuracy, robustness and resiliency throughout the development process and adapt the designs when required thresholds are not met)

The provider has to keep things like the technical documentation or the documentation regarding the QMS available for national authorities for at least 10 years after the system has been placed on the EU market. [3, Chapter 3, Article 18] (**AI.PR9:** Provider of a high-risk AI system has to keep technical documentation; documentation on the QMS; documentation of the changes; documentation of de-

cision of notified bodies and EU certificate of conformity for at least 10 years from the moment when the AI system was placed on the market)

High-risk AI systems are allowed to generate logs automatically for the duration of its lifetime. These logs have to include events where the system may cause a risk to occur. The logs also need to include events that are relevant for post-market monitoring and monitoring the operation of the AI system. [3, Chapter 3, Article 12] Article 19 describes how these logs need to be kept for an appropriate amount of time that is at least six months. [3, Chapter 3, Article 19] (**AI.PR10:** Automated logs of a high-risk AI system need to be kept for a period appropriate to the intended purpose of the high-risk AI system that is at least six months)

If the provider thinks that or has a reason to think that the high-risk AI system is no longer in conformity with the AI Act, they have to immediately start all the necessary corrective actions to bring the system back into conformity. The provider also needs to inform the distributors, deployers and relevant authorities and other possible parties like importers of the system. [3, Chapter 3, Article 20] If the high-risk AI system presents a risk to health, safety or the fundamental rights of persons, the provider has to immediately start investigation to find the cause for this risk and inform possible deployers and relevant authorities that have issued a certificate for the system. [3, Chapter 3, Articles 20 and 79] (**AI.DR4:** Provider of a high-risk AI system has to keep vigilant watch over the system and take immediate action if the system is not in conformity with the AI Act. This action has to include measures to make the system conform to the AI Act again and also measures to notify all the required parties)

Article 21 describes how the provider of a high-risk AI system has to able to show authorities on request that the AI system is in conformity with the AI Act. Authorities must also be allowed access to the automated logs of the system. (**AI.DR5:** Provider of a high-risk AI system has to have at all times a clear picture of, is the

system in conformity with the AI Act. Provider of the system has to also be able to prove it on request)

For each high-risk AI system that the provider has, they need to draw up an EU declaration of conformity and keep it available for relevant authorities for 10 years after each system has been placed on the market or put into service. Each declaration has to identify which high-risk system it has been drawn up for. The declaration has to state that the system it is assigned to meets all the relevant requirements of the AI Act. By drawing up a declaration of conformity, the provider takes responsibility in making sure that the system does indeed conform to the AI Act. [3, Chapter 3, Article 47] (**AI.PR11:** Provider of a high-risk AI system has to draw up an EU declaration of conformity for each AI system that they have)

4.3.3 Transparency obligations and General-purpose AI systems

Chapter 4 of the AI Act describes all the transparency obligations of providers and deployers. The first obligation of the chapter is about the providers of AI systems that interact directly with natural persons. Providers need to inform the natural persons that they are interacting with an AI system unless it is obvious to reasonably well-informed person. [3, Chapter 4, Article 50, Paragraph 1]

Providers of AI systems that synthetic audio, image, video or text content have to make sure, that all the generated content is marked in a machine-readable format and that the content is identifiable as AI generated or manipulated. This obligation does not affect AI tools that assist in standard editing process or AI systems that do not significantly alter the input data. [3, Chapter 4, Article 50, Paragraph 2] (**AI.PR12:** All AI generated or manipulated content has to be marked as synthetically generated) Providers also have to ensure that their technical solutions are "effective, interoperable, robust and reliable as far as this is technically feasi-

ble" [3, Chapter 4, Article 50, Paragraph 2] (**AI.DR6:** Providers of AI systems that generate content have to make sure that their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible)

Providers of general-purpose AI models that meet or are going to meet the conditions for high impact capabilities and therefore be deemed to be a system with systemic risk, have to inform the EU commission on the matter. The note to EU commission has to be sent without delay and by latest two weeks after the conditions are met or become known that they are going to be met. The note must contain information necessary to demonstrate that the relevant conditions have been met. [3, Chapter 5, Article 52, Paragraph 1]

The provider may present arguments with the note, that despite the AI system meeting the requirements, it does not present systemic risk due to its characteristics or other factors. The EU commission will then go through the arguments and decide based on the evidence if the general-purpose AI system is a system with systemic risk. [3, Chapter 5, Article 52, Paragraphs 2 and 3] (**AI.PR13:** EU commission must be informed within two weeks after the system meets the requirements, or it becomes known that the system will meet the requirements for a high impact system)

As **AI.PR13** gives a tight deadline for notifying authorities on the high impact capabilities of the system, the provider of the general-purpose AI system has to consistently measure and be aware of the capabilities of the system. Considering that the AI Act mandates the providers overall to notify authorities in certain situations, the requirement for constant measurement and evaluation of AI systems does not limit to just general-purpose AI systems. (**AI.DR7:** Providers of AI systems must consistently measure and be aware of the AI system´s capabilities)

Article 53 lists the obligations that providers of general-purpose AI models must meet. These providers must create and keep up-to-date technical documentation

of the AI model. [3, Chapter 5, Article 53] The documentation must contain at minimum all the topics mentioned in the Annex XI of the AI Act. These topics range from general description of the AI model like the tasks that the model is intended to perform and the type and nature of AI systems in which it can be integrated to, and the design specifications of the model and its training process. [3, Annex XI] (**AI.PR14:** Providers of general-purpose AI systems must draw up and keep up-to-date technical documentation of the AI system)

Article 53 also obligates providers to create documentation for other providers who will integrate the general-purpose AI model to their own AI system. This documentation must include at least all the elements mentioned in Annex XII. The documentation's goal is to *"enable providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model and to comply with their obligations pursuant to this Regulation"* as it is stated in the AI Act. [3, Chapter 5, Article 53] (**AI.PR15:** Providers of general-purpose AI systems must draw up and keep up-to-date documentation for providers who intend to integrate the general-purpose AI system into their own AI system)

These two document sets that are stipulated by **AI.PR14** and **AI.PR15** must be drawn up by the provider of a general-model AI system. For this to be possible, the provider needs to decide what tasks are the AI system supposed to do and what are its capabilities and limitation within the parameters of those tasks. The provider also needs to define use policies for the use of the AI system among all the other elements for the system to be compliant to the regulations. (**AI.DR8:** Provider of a general-purpose AI system must decide the tasks that the AI is fit to be used in and write those tasks down for the possible users and deployers of the AI system)

Section 3 of legislation regarding general-purpose AI models lists additional requirements that providers of AI models with a *systemic risk* have to fulfil. These providers must conduct model evaluations with standardised protocols and tools.

These evaluations also need to include adversarial testing, where the aim is to identify and mitigate systemic risks. [3, Chapter 5, Article 55] These providers are also obligated to assess and mitigate possible systemic risks that may arise from development or use of the AI system in the EU market. The article specifically mentions that this assessment should be done at EU level. They are also mandated to document and inform the AI Office about serious incidents. These providers are also advised to provide suggestions to remedy these types of incidents. AI systems with systemic risk must also have an *"adequate level of cybersecurity protection"* [3, Chapter 5, Article 55] (**AI.PR16:** Providers of general-purpose AI systems with systemic risk must try and mitigate those systemic risks by means of conducting model evaluations; maintaining an adequate level of cybersecurity; notifying and advising the AI Office of serious incidents and systemic risks at the EU level)

The *post-market monitoring system* has to be established for any and all high-risk AI systems and the monitoring system has to be proportional to the risks and the nature of the system. This monitoring system will collect, document and analyse the performance of the AI system throughout its lifetime. This monitoring system has to be based on a *post-market monitoring plan*, which is one of the documents that needs to be part of the mandatory technical documentation. [3, Chapter 9, Article 72] (**AI.PR17:** Providers of high-risk AI systems need to create a post-market monitoring plan and then follow it with the post-market monitoring system)

4.3.4 Testing AI systems

In Chapter six of the AI Act, the means of conducting tests of high-risk AI systems in real-world conditions outside the *AI regulatory sandbox* are described. This real-world testing is allowed if all 11 of the listed preconditions are met. These conditions necessitate the creation of a *real-world testing plan* and it needs to be accepted by relevant national authorities. [3, Chapter 6, Article 60, Paragraph 4]

(**AI.PR18:** Providers of high-risk AI systems that aim to test their systems in real-world conditions must create a real-world testing plan)

The real-world testing can only last as long as it is necessary, however the absolute maximum amount of allowed time is six months. This six-month time limit can be extended with another six months, but the extension must be justified, and the justifications must be provided to the relevant national authorities who decide if the extension is granted. [3, Chapter 6, Article 60, Paragraph 4] Freely given consent must be given by the data subject before their data can be used in the real-world testing. The results of the testing in the real-world conditions cannot have negative effects on the data subjects, and their personal data has to be deleted after the test. [3, Chapter 6, Article 60, Paragraph 4] (**AI.DR9:** The provider of an AI system must carefully consider what they want to test and plan accordingly to ensure that the possible risks and adverse outcomes to the data subject are minimised)

5 Interviews

5.1 Background

As the aim of this thesis is to find new requirements that recent EU regulations have put upon software development, this thesis utilises interviews to make sure that the requirements found in the literary analysis are actual requirements that affect software development. The interviews also help find other requirements not noticed in the literary analysis.

The interviews were conducted at Company X, which operates in the finance sector in Northern Europe and it employs more than 1000 employees in IT related tasks. This company uses a modified Agile framework for its software development, where they utilise events like *Sprints* and *Supersprints*.

5.2 Interview setting

The interviews are semi-structured around a set of interview questions that the interviewees answer freely with their own words, with the exception of Question Q8, where they had to select and answer from three different options. The interviews were conducted individually, giving each interviewee the chance to explain their views and opinions more in-depth. The interviews were conducted in an online video conference platform, where only the audio of these interviews was recorded. The total length of these records is 3 hours. The interviews were held in April 2025.

The interviews were conducted in Finnish or English based on the preference of the interviewee. The interview questions were translated to Finnish if it was requested by the interviewee. Additionally, the answers were translated into English if the interviewee answered in Finnish.

5.2.1 Selection of the interviewees

The goal for the selection of the interviewees was to have them come from multiple different roles and responsibility areas to increase the possibility for different perspectives to the interview questions. Five interviews were conducted in total, and the backgrounds of the interviewees can be seen in **Table 5.1**. Fifteen people were contacted in total to ask if they would be willing to be interviewed, but ten people refused citing the lack of knowledge on relevant legislation or their busy schedule.

5.2.2 Interview questions

Interview questions are listed in **Appendix A**. The questions were sorted into three different segments: *Background*, *EU regulations*, and *Compiled requirements*. The first segment – *Background* – aims to provide context to the answers of each interviewee, as the questions ask things like, job title, amount of experience in the field, and do they have experience in dealing with different EU regulations.

The second segment is *EU regulations* and its aim is to find out what effects EU regulations like GDPR, DORA and AI Act have the interviewees noticed in their line of work. Other questions in this segment are: *Do you think Company X is compliant with the AI Act, GDPR, and/or DORA at the moment and in the near future?*; and *How do you think AI is utilised at the moment and in the near future in Company X?*

The third and final segment is *Compiled requirements*, where the requirements collected from Chapters 3 and 4 were presented to the interviewees. These require-

ments were collected and presented to the interviewees in the form of **Appendix B**. In Q8, the interviewees were asked to answer the question *"Given this list of requirements compiled from the GDPR and AI Act, do these requirements cause any changes to the way Company X operates?"* with one of the following options: *does not cause changes*; *somewhat causes changes*; and *causes a lot of changes*. The interviewees gave their answers to a single requirement from the list at a time. The interviewees were allowed to expand on their answers and on some occasions, they were asked to explain their answers to a specific requirement.

5.3 Interview results

5.3.1 Background

The first segment of the interview asked the basic information of the interviewees. The answers to Q1 showed that the interviewees came from different teams and areas of software development and also from different steps of organisation in Company X from developer to tribe lead and head of a division. All interviewees have a long history in software development as the shortest time in the field was 12 years among the interviewees. However, in their current roles the interviewees have been between 1 and 6 years. Their job titles and brief summaries of their job descriptions are listed in **Table 5.1**.

All interviewees except *I2* have had experience in dealing with *GDPR* and *DORA*. This greatly contrasts with the fact, that none of the interviewees had experience in dealing with *AI Act*. This is expected, as Company X does develop its own AI systems, but the development process is at the moment very concentrated in certain development teams, so other personnel are not that familiar with AI development and regulations that affect it.

The background of the interviewees also gives insight that organisational roles

Table 5.1: The interviewees

	Experience (years)	Work description
I1	13	Creation and maintenance of the Engineering handbook and the mapping of requirements in DORA
I2	15	Development and maintenance of tools for internal end-users
I3	12	Tribe lead of an Agile development tribe
I4	27	Responsibilities in IT security functions
I5	17	Fixing technical, organisational and inter-personal problems in all engineering teams

that deal with designing systems and leading teams of developers forces them to deal with EU regulations. This makes it so that developers do not need to actively think about EU regulations, as they are given internal rules and guidelines to follow instead of following the articles of EU regulations. *I2* says the following on their experiences with DORA and AI Act:

> *"I did not even hear about DORA until couple months ago, when I was tasked to creating some disaster recovery plans and I know AI Act only through media. We don´t deal with a lot of AI stuff in my current position."*

This quote shows that, even if the principles and requirements of an EU regulation are adopted in a company, the reason for these changes might still remain unknown to some personnel, due to the fact that some personnel were handed tasks to develop single functionalities or changes to software without necessarily specifying that they were due to DORA.

I3 remembered that they were working in a slightly different job at the time and

they were a bit more directly involved in dealing with the GDPR when it was first adopted. They said the following:

> *"When these regulations were put into effect, I was in a role where I had to create documentation and do mapping with the developers. In my current role, I am dealing with a bigger picture so that we can meet expectations (from regulations) and so that we can make sure that ownerships and activities are clear."*

I4 had similar experiences with GDPR and DORA, but not with AI Act. They mentioned the following:

> *"A couple years before GDPR was put into effect, we had a GDPR Project. I was in a steering group for those couple years, especially with the security controllers. And now with DORA it has been the same story with me."*

5.3.2 EU regulations

EU regulations was the title in Appendix A for interview Questions Q4-Q7, which asked more questions on, what changes these regulations have caused and how Company X has dealt with them in general. It also asked a question on how much AI is utilised in Company X at the moment.

In general terms, GDPR and DORA did cause some changes in how Company X conducts software development. *I1* describes the nature of changes in a following way:

> *"Though I would say two third of those things are the same that we've been doing before. There is more stricter rules which are applying starting from now and that affects of course teams and squads, because they*

> *have to, first of all, go through all of their assets to understand what is compliant, what is not. This is their big task."*

I1 also discussed the changes, that DORA caused to testing and how should companies think about testing. *I1* noted, that before everyone was aware of quality assurance, but not all had thought about organisations having key experience in testing. DORA has changed this and now companies have to also think about testing strategies.

I1 recognised that EU has included requirements in the regulations that have been previously considered internal quality requirements and internal practises. All other interviewees agreed with this opinion when they were asked about that insight. *I3* mentioned:

> *"When regulations are brand new, it takes a long time in each team to understand what needs to be done (. . .) It requires that an organisation has to have a level of coordination in it but in lower team and squad level, they must make sure that the required actions are done always and they are kept memorised."*

I3 Also noted that Company X had some issues with coordinating the adoption of DORA when it was preparing for the date when DORA came into effect. The issues revolved around the fact, that some teams were trying to solve the same problems without knowing that other teams were also trying to find a solution for those same problems. This may have been because of a lack of clear coordination, but in later stages this was fixed.

I5 agreed on that these regulations have indeed caused changes to their and their teams work, but they wanted to add the following:

> *"Finance sector is already heavily regulated, and I want to ask, have the basic principles even really changed that much after these regulations*

were put into effect? Maybe these things (data protection etc.) are just more in the limelight than before."

All the interviewees had slightly different ideas or viewpoints on the use of AI systems in Company X. In general, the interviewees were not aware, that Company X is developing AI systems at the moment. Company X does have some pilot trials with Microsoft Copilot 365 licenses in order to determine in what business areas its usage would be useful. Company X has set up an organisation called the AI Center of Excellence, and its task has been mapping all the potential tasks that could be improved or handled by AI. *I2* said:

"We use Copilot as a tool sometimes. We don´t have a lot of confidence in it, actually. Sometimes we use ChatGPT to help us figure something out. Asking ChatGPT is usually faster than reading through forums like Stack Overflow looking for answers that might not be what you are looking for."

Question Q7 provided interesting insights on the nature of regulatory compliance. All the interviewees agree that Company X is very compliant with the regulations that affect it. Interviewees pointed out, that in their personal opinion, Company X does not necessarily need to be 100% compliant. This is because of some of the requirements that are in the regulations are very open-ended and not explicit, making some aspects of them quite depended on who is interpreting the text. *I5* said the following:

"Company X is mostly compliant with these regulations. (...) I am not certain if Company X is compliant with AI Act or FIDA (Framework for financial data access)."

I4 also commented on the difficulty of being 100% compliant. Difficulties arise in the Articles that are not well-defined:

"It is very difficult to be 100% compliant, but with what I have been a part of, I can say that Company X has gone very far with the process."

I1 also pointed out that there is a grey area in being compliant. They argue, that having a plan while not being compliant is much better than not even having a plan on how to become compliant:

"We discussed with our Tech risk, Compliance, and Legal teams what we know what DORA is about and what is required with our Compliance and Legal teams. We mapped it to our assets. We know the gaps and we have an active plan how to fix it in the upcoming one year."

I3 also mentioned, that it might not be in the interest of a company to be 100% compliant, as the final changes that affect very little require proportionally extremely large amounts of work and resources. Their quote is as follows:

"Company X is a company that wants to be compliant. It might not necessarily be compliant on every little detail or small service but with larger risks it is compliant, like with systems that process sensitive personal data. (...) My own opinion is that if you want to be 100% compliant with regulations, then you have done a bit too much."

5.3.3 Compiled requirements

The final segment of the interview dealt with the requirements that were collected in Chapters 3 and 4 and listed in Appendix B. Interviewees answered to each single requirements separately and their answers are presented in **Figures 5.1-5.5**. *I2* was not able to answer these due to the lack of knowledge on how these requirements would change the way Company X operates. *I4* and *I5* both had a few singular requirements that they were not able to answer in the requirements set by AI Act due to the lack of knowledge on the topic. All of these answers were removed from

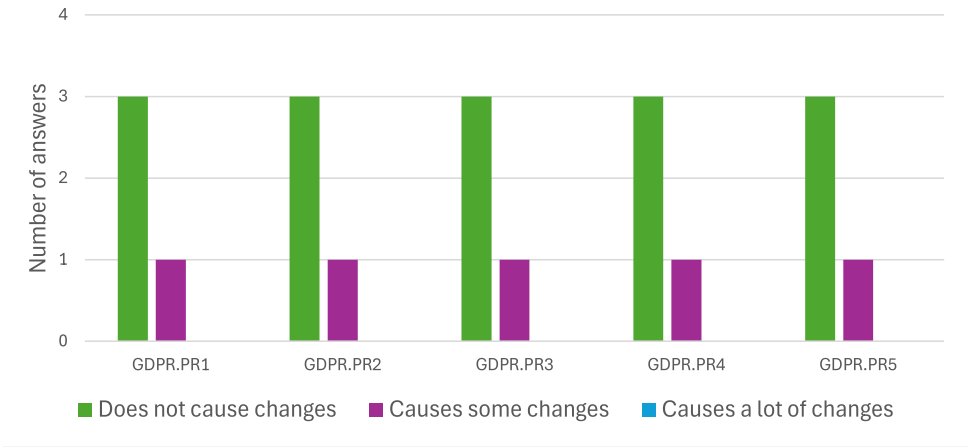

Figure 5.1: Answers to the GDPR.PR requirements

the collected data and thus they are not included in the figures showing the different answers.

In the first set of requirements that all deal with *PR* requirements of GDPR the majority of interviewees said that Company X is already compliant for the most part. Each of them answered "Causes some changes" to one or two of the requirements with each mentioning that some legacy systems might not fully comply with the requirement in question at that moment. Answers are presented in **Figure 5.1**. *I5* gives the following example:

> *"We have three silos that correspond with different business areas. We have also created our system architecture to be very location based, which has caused us to have 3 similar systems that all do the same thing but possibly with some very minor differences between them. (...) Even if Company X does not actually have these kinds of duplicates, we should still prepare for those and that causes some changes in the way we operate."*

The second set of requirements were the *DR* requirements of GDPR. In this section the interviewees answered similarly that Company X is already compliant, and these requirements do not cause a lot of changes. The only exception was *I5*,

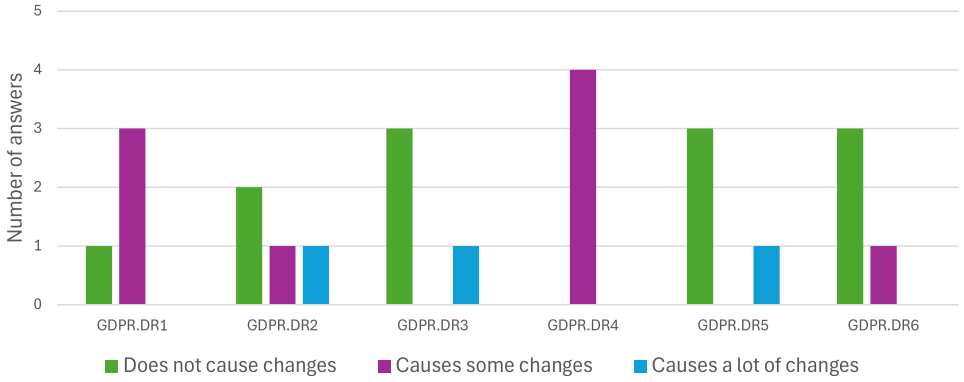

Figure 5.2: Answers to the GDPR.DR requirements

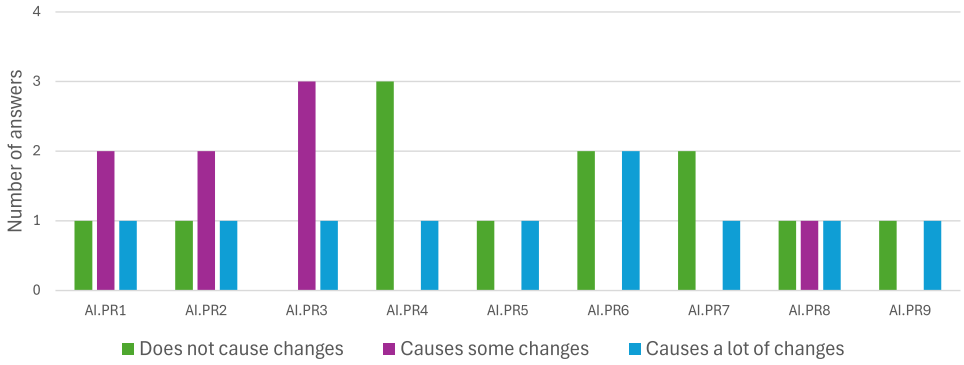

Figure 5.3: Answers to the AI.PR1-AI.PR9 requirements

who answered, that requirements *GDPR.DR2*, *GDPR.DR3*, and *GDPR.DR5* cause a lot of changes. *I5* justified their reasoning on the fact that Company X does not have an unified way, that everyone follows. Each team does these required things in their own way, which caused the answers of *I5* to be "Causes a lot of changes". The answers to *DR* requirements of *GDPR* are presented in **Figure 5.2**.

The segment with the most requirements was the *PR* requirements of the *AI Act*. This segment had more variance in answers between the interviewees due to the fact that the interviewees have not been in projects within Company X that deal with the development of AI systems, so the interviewees were not as familiar with the requirements, and they interpreted them in slightly different ways. The answers to this segment are presented in **Figure 5.3** and **Figure 5.4**.

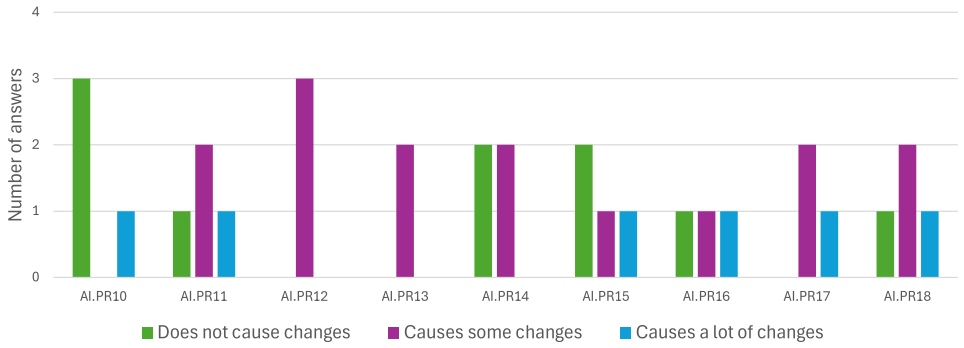

Figure 5.4: Answers to the AI.PR10-AI.PR18 requirements

In general, the consensus is that it would be a momentary hurdle to set up all these required things, but Company X already has dealt with regulations that deal in similar topics, only in different business contexts. Therefore *I3* answered that the requirements would cause a lot of changes. *I1* and *I5* both agreed that they do cause some changes, but *DORA* has forced Company X to make changes that would make it already compliant with *AI Act* if the systems and practises in developing AI systems would be build up with them in mind. *I1* said the following:

> *"Maybe less on the effort because I would say it goes hand in hand with DORA. So, if we do it for DORA, for any AI system, it would automatically apply. (...) It's quite interesting to see that it has so many correlations with DORA. And as I said, it only hit me after some time that DORA is not required for a lot of companies. It's only for the specific insurance, banking and investment portfolios companies."*

I3 said the following on, why they think that almost all of the requirements require a lot of changes in their opinion:

> *"If we now start to build an AI solution, it would definitely be a big effort because we do not have know-how or experience in our different teams. We would need to build competence first to these teams."*

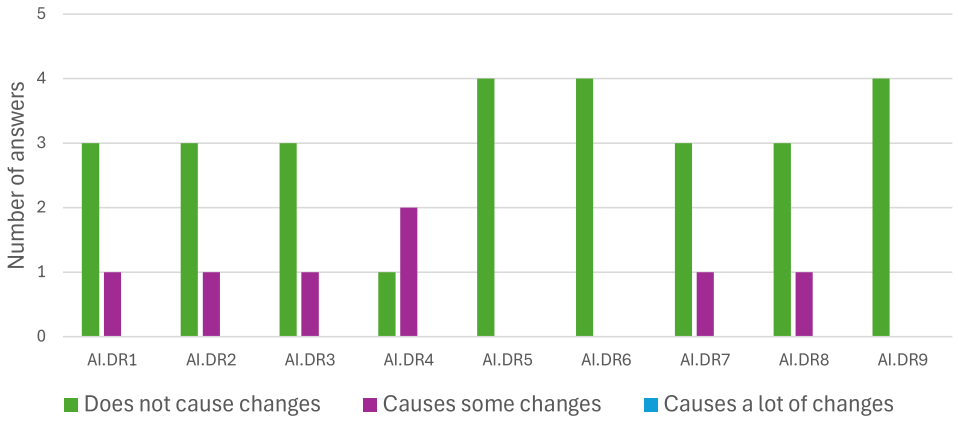

Figure 5.5: Answers to the AI.DR requirements

The last segment of requirements were the *DR* requirements of *AI Act*. The interviewees were much more confident with their answers on these requirements. Their opinion was that Company X is already quite compliant with these requirements, but some work would need to be done to be fully compliant. The answers to this segment are in **Figure 5.5**.

I1 said all these are requirements that can be found in *DORA* in some form, so the requirements are mostly already covered by Company X. One exception was *AI.DR4*, which requires the provider of a high-risk AI system to keep vigilant watch over the system and take action if it is not in conformity with regulations. Company X does comply with this requirement, but some not business-critical systems might not have 24/7 surveillance on them.

Other interviewees also pondered the requirement of vigilant watch, and they were not sure what level of system surveillance is enough. The same questions also arose in requirements *AI.DR1-AI.DR3*. Regardless they estimated that Company X would have enough surveillance to be considered compliant with these requirements. *I5* summarised their thoughts in the following way:

> *"I think that these do not cause changes as I consider these to be just good practises that we already do."*

Q9 and Q10 were asked at the end of the interviews, and the answers were similar with all of the interviewees. The requirements seemed reasonable, but some needed specifics were missing. *I2* thought that EU has taken a good direction in including some of the quality best practises in regulations. No additional requirements were proposed by the interviewees.

6 Conclusions and further work

6.1 Discussion

This thesis had two research questions, RQ1 and RQ2, that asked what changes do recent EU regulations cause to software development and how these changes are achieved. The literature analysis produced a list of requirements that were split into two categories, PR and DR.

Product Requirements (PR) of GDPR showed, that data processing must be recorded, and in general the data must be able to be either removed or made anonymous. This means, that the developer of a system that handles personal data must consider what data will be used and for what purposes and is that data subject to the right to become forgotten. The Development Requirements (DR) found from GDPR laid out rules that make the developer be more prompted to design systems with data protection in mind and have structures in the development process that reflect on the process and improve it when some things or aspects are found lacking.

The PR and DR requirements from AI Act also paint a similar picture but just in a different context. The base idea is to create structures via regulations that help the developers to consider, what can and will go wrong in the development process or in the developed system. That is why the regulations add requirements for Quality management systems for high-risk AI systems for example. Other aspect that these requirements enforce, is that the developers have to know what the developed system

can do at the moment, and they have to evaluate is that enough or too much for the tasks that the system is designed to accomplish.

The interviews also provided answers that correlated with these findings from the literary analysis. There seems to be a trend, where EU tries to insert new requirements to its regulations that were previously considered to be good practises and other self-policed quality requirements of the industry. This seems to cause some overlap in the ideas and goals of different EU regulation packages. Like *I1* mentioned in the interviews, similar requirements are set by sections of DORA and AI Act.

The interviewees agreed that the requirements that the regulations form are reasonable and justified in general, but some of the specific Articles in those regulations are too open-ended for defining clearly what needs to be done in order to achieve compliance. These uncertainties require companies to turn to internal legal teams or to external law offices to find out what actually is required in order to be compliant, thus slowing down the complete adoption of these regulations and possibly incentivising the developers to cut corners and not follow regulations due to the high cost of adoption and uncertainty of what is enough to be compliant.

These requirements are complex, and they affect almost every aspect of software development. Interviews also pointed out that there must be a separate level on the organisation that can coordinate the adoption of new procedures and methods of working. DORA did cause challenges with Company X and some of those challenges stemmed from the lack of coordination, where different teams tried to solve the same problems without knowledge that others were also dealing with the same problem.

Companies also need to build up competence in the technology that they develop. That is another hurdle that all companies must cross in order to be successful and compliant with relevant regulations. It means that it is not enough to just follow what the regulations say, but you must also consider what skills do the personnel of

a company need in order to ensure that the development process is efficient and the results are compliant.

6.2 Conclusions

RQ1 of this thesis is: *What changes do the recent EU regulations cause to Software Development methods?* The data collected from the literature analysis and the interviews shows that the recent EU regulations cause a myriad of changes to software development methods. The data from the literature analysis was collected into a list of requirements that were split into two different categories, PR and DR. The regulations mandate the creation of new management systems, like the Quality management system, to make the developed systems to have more measures within them to make them be less risky to cause harm to data subjects or end users or other parties related to the systems.

The developed systems must also include measures to limit the processing of sets of data or even delete the data if it needed. These situations can arise from sources like lawful requests by data subjects. The developed programs and systems must also include measures to make them as resistant to internal and external faults and threats as is reasonable considering the what the systems is used for. The EU regulations also included requirements to develop the systems with as state-of-the-art techniques and technologies as is appropriate considering the scope and the nature of the system and its data processing.

The interviewees summarised that the recent regulations contain concepts that have been previously considered to be good development practises. These good practises have not been monitored by national authorities before these regulations and the adoption of those practises can cause trouble for some companies. Company X did follow these good practises before, so these regulations did not cause a lot of trouble for Company X regarding Articles that introduce these good practises as

required techniques and methods in order to be compliant with regulations.

These good practises are requirements like knowing the capabilities of a system and documenting the intended use cases of the system communicating those things clearly to the users of the system. Other good practises are commenting what a piece of a program does and creating plans for testing the system in order to ensure that the tests are as comprehensive as possible.

The regulations in the AI Act naturally only affect AI systems and companies that develop AI systems, but similar principles are included in other EU regulation packages, like DORA where the regulations affect companies in the finance sector. EU seems to want to enforce certain ways of development to ensure that the developed systems maximise things like data protection of EU citizens, but it tweaks these general principles to each different niche of development.

RQ2 of this thesis asked the question *How are the necessary changes accomplished?* The collected data suggests that companies need to be aware what EU is planning and what types of legislative packages are on the horizon for the near future. They need to be pre-emptively planning on what changes they need to make in order to prepare for the moment then the EU proposals become regulations that are in effect. This process contains phases like mapping the requirements into business functions or development phases and assigning responsibilities to specific teams or single members of the company organization.

Companies will find problems if there are no organisational structures or teams that coordinate the process of making changes in order to become compliant. If there is no coordination, large amounts of effort will be wasted because different teams will try to solve the same problems and in the worst cases, they will create solutions that are not compatible with each other. Disjointed solutions can also cause the company to not be compliant with the regulations due to the inconsistent solutions between different teams and business units.

6.3 Research limitations

The limitations of this thesis leave some questions unanswered on this topic and further research is required. This thesis thoroughly analysed only the EU regulations of GDPR and AI Act, from which the list of requirements was generated. DORA was partly analysed. Its contents were not dissected and listed into requirements, as it was only introduced and explained in order to give context on some of the interviews due to it being one of the most recent regulations related to the subject of this thesis.

The choice of focusing on the AI Act caused some issues with this thesis as AI development in Company X is very focused on certain teams, making other teams at Company X to not be aware of it. That caused some interviewees to not be so certain on how they should interpret each question and requirement. It also caused some of the people to not want to take part with the interview. That lead to one other limitation of this thesis, and it is the low number of interviewees. Preferably there should have been more interviewees as it would have given more data to this thesis and most likely additional viewpoints and insights to the interview questions.

Another limitation also is that this thesis only interviewed people from one company. Software development changes from one company to another and the chosen company only develops software for its own use only. Additional insight to the research questions would have been possible if interviews would have been extended to other companies that develop software. It would also increase the possibility where a company would have had experiences in being less prepared into adopting EU regulations and thus given more knowledge on what situations need to be avoided to ensure successful adoption of EU regulations.

6.4 Further research

This topic needs additional research, and it can be done with different selections of EU regulations and target companies. As pointed out in Section 6.3, interviewing people from multiple different technology companies would give a more comprehensive understanding on what need to be considered when planning for changes. Preferably these companies would produce software for different purposes and with different levels of needed personal data. The current trend of AI development and the future maturation of the AI as a technology will also provide ample sources for additional research and research questions.

The other way additional research on this topic could be conducted is to wait a bit to give Company X some time to completely adopt the planned changes to DORA and other recent regulations and conduct a follow-up interview on have their views changed and did the plans work as intended.

References

[1] "Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 december 2022 establishing the Digital Decade Policy Programme 2030", *Official Journal of the European Union*, pp. 4–26, L 323/4 2022, ISSN: 1977-0812.

[2] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)", *Official Journal of the European Union*, pp. 1–88, L 119 2016, ISSN: 1977-0677.

[3] "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 june 2024 laying down harmonised rules on artificial intelligence and amending regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and directives 2014/90/eu, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)", *Official Journal of the European Union*, L 2024/1689 2024, ISSN: 1977-0677.

[4] C. Vander Maelen, "Hardly law or hard law? investigating the dimensions of functionality and legalisation of codes of conduct in recent EU legislation and the normative repercussions thereof", *European Law Review*, vol. 47, no. 6, pp. 752–772, 2022.

[5] "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011", *Official Journal of the European Union*, pp. 1–79, L 333 2022, ISSN: 1977-0677.

[6] K. Petersen, C. Wohlin, and D. Baca, "The waterfall model in large-scale development", in *Product-Focused Software Process Improvement: 10th International Conference, PROFES 2009, Oulu, Finland, June 15-17, 2009. Proceedings 10*, Springer, 2009, pp. 386–400.

[7] C. Larman, *Agile and iterative development: a manager's guide*. Addison-Wesley Professional, 2004.

[8] N. B. Ruparelia, "Software development lifecycle models", *SIGSOFT Softw. Eng. Notes*, vol. 35, no. 3, pp. 8–13, May 2010, ISSN: 0163-5948. DOI: 10.1145/1764810.1764814.

[9] J. Morris, *Software industry accounting*. John Wiley & Sons, 2001, ISBN: 9780471437451.

[10] A. M. Langer, *Guide to software development : designing and managing the life cycle*, eng, Second edition. London: Springer, 2016, ISBN: 9781447167990.

[11] P. Ralph and Y. Wand, "A proposal for a formal definition of the design concept", in *Design Requirements Engineering: A Ten-Year Perspective*, K. Lyytinen, P. Loucopoulos, J. Mylopoulos, and B. Robinson, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 103–136, ISBN: 978-3-540-92966-6.

[12] A. M. Davis, *201 principles of software development*. USA: McGraw-Hill, Inc., 1995, ISBN: 0070158401.

[13] J. Bøegh, "A new standard for quality requirements", *IEEE Software*, vol. 25, no. 2, pp. 57–63, 2008. DOI: 10.1109/MS.2008.30.

[14] R. L. Glass, *Facts and fallacies of software engineering*. Addison-Wesley Professional, 2002.

[15] C. Kaner, "Exploratory testing [PowerPoint slides]", Quality assurance institute worldwide annual software testing conference, 2006.

[16] C. Kaner, J. Falk, and H. Q. Nguyen, *Testing computer software*. John Wiley & Sons, 1999.

[17] T. Baum, O. Liskin, K. Niklas, and K. Schneider, "Factors influencing code review processes in industry", in *Proceedings of the 2016 24th acm sigsoft international symposium on foundations of software engineering*, 2016, pp. 85–96. DOI: 10.1145/2950290.2950323.

[18] M. V. Mäntylä and J. Vanhanen, "Software deployment activities and challenges - a case study of four software product companies", in *2011 15th European Conference on Software Maintenance and Reengineering*, 2011, pp. 131–140. DOI: 10.1109/CSMR.2011.19.

[19] G. Canfora and A. Cimitile, "Software maintenance", in *Handbook of Software Engineering and Knowledge Engineering: Volume I: Fundamentals*, World Scientific, 2001, pp. 91–120.

[20] W. W. Royce, "Managing the development of large software systems: Concepts and techniques", in *Proceedings of IEEE WESCON*, IEEE Computer Society Press, 1970, pp. 1–9.

[21] L. R. Vijayasarathy and C. W. Butler, "Choice of software development methodologies: Do organizational, project, and team characteristics matter?", *IEEE Software*, vol. 33, no. 5, pp. 86–94, 2016. DOI: 10.1109/MS.2015.26.

[22] B. Boehm, "A spiral model of software development and enhancement", *ACM SIGSOFT Software engineering notes*, vol. 11, no. 4, pp. 14–24, 1986.

[23] B. W. Boehm and W. J. Hansen, "Spiral development: Experience, principles, and refinements", 2000.

[24] N. M. A. Munassar and A. Govardhan, "A comparison between five models of software engineering", *International Journal of Computer Science Issues (IJCSI)*, vol. 7, no. 5, p. 94, 2010.

[25] K. Beck, J. Grenning, R. C. Martin, M. Beedle, J. Highsmith, S. Mellor, A. van Bennekum, A. Hunt, K. Schwaber, A. Cockburn, R. Jeffries, J. Sutherland, W. Cunningham, J. Kern, D. Thomas, M. Fowler, and B. Marick, "Manifesto for agile software development", 2001.

[26] "Examining the Agile Manifesto: Think outside the Agile box", `https://www.ambysoft.com/essays/agileManifesto.html`, last seen 23.3.2025.

[27] K. S. Rubin, *Essential Scrum: A practical guide to the most popular Agile process*. Addison-Wesley, 2012.

[28] K. Beck, "Embracing change with extreme programming", *Computer*, vol. 32, no. 10, pp. 70–77, 1999. DOI: `10.1109/2.796139`.

[29] K. Schwaber, *Agile project management with Scrum*. Microsoft press, 2004.

[30] J. Sutherland, "Agile development: Lessons learned from the first scrum", *Cutter Agile Project Management Advisory Service: Executive Update*, vol. 5, no. 20, pp. 1–4, 2004.

[31] J. Winn and N. Jondet, "A "new approach" to standards and consumer protection", *Journal of consumer policy*, vol. 31, pp. 459–472, 2008.

[32] P. G. Chiara, "The IoT and the new EU cybersecurity regulatory landscape", *International Review of Law, Computers & Technology*, vol. 36, no. 2, pp. 118–137, 2022. DOI: `10.1080/13600869.2022.2060468`.

[33] E. Rotondo, "The legal effect of EU regulations", *Computer Law & Security Review*, vol. 29, no. 4, pp. 437–445, 2013, ISSN: 0267-3649. DOI: 10.1016/j.clsr.2013.05.003.

[34] "Consolidated version of the treaty on the functioning of the European Union", *Official Journal of the European Union*, pp. 171–172, C 326/1 2012, ISSN: 1977-0677.

[35] R. Rajala, "Liike-elämän odotukset opiskelijoiden tietoturvan osaamiselle [PowerPoint slides]", Finnish Information Security Cluster, 2024.

[36] F. Terpan, "Soft law in the european union—the changing nature of EU law", *European Law Journal*, vol. 21, no. 1, pp. 68–96, 2015. DOI: 10.1111/eulj.12090.

[37] J. Wu and M. Hayward, "International impact of the gdpr felt five years on", https://www.pinsentmasons.com/out-law/analysis/international-impact-of-the-gdpr-felt-five-years-on, last seen 4.3.2024.

[38] A. Jones, "GDPR three years later: What impact has it made?", https://www.ispartnersllc.com/blog/gdpr-one-year-later-impact/, last seen 4.3.2024.

[39] R. Rughiniș, C. Rughiniș, S. N. Vulpe, and D. Rosner, "From social netizens to data citizens: Variations of GDPR awareness in 28 european countries", *Computer Law & Security Review*, vol. 42, p. 105 585, 2021, ISSN: 0267-3649. DOI: 10.1016/j.clsr.2021.105585. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364921000583.

[40] "Digital Operational Resilience Act (DORA)", https://www.eiopa.europa.eu/digital-operational-resilience-act-dora, last seen 27.2.2025.

[41] "EU AI Act: First regulation on artificial intelligence", https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence, last seen 22.9.2024.

[42] T. Madiega, "General-purpose artificial intelligence", *At a Glance*, PE 745.708 2023.

Appendix A Interview questions

Background

Q1: What is your job title and description?

Q2: How long have you been at your current job and how much do you have work experience in your field in general?

Q3: Do you have any experiences in dealing with EU regulations like GDPR or DORA?

EU regulations

Q4: Have you noticed any changes that affected your or your team´s work practises after GDPR, DORA, or AI Act were put into effect?

Q5: Has your work been affected by the AI Act, GDPR and/or DORA?

Q6: How do you think AI is utilised at the moment and in the near future in Company X?

Q7: Do you think Company X is compliant with the AI Act, GDPR, and/or DORA at the moment and in the near future?

Compiled requirements

A list of compiled requirements (Appendix B) from the literary review was provided to each interviewee prior to the interview.

Q8: Given this list of requirements compiled from the GDPR and AI Act, do these requirements cause any changes to the way Company X operates?

Q9: Do you think any of these requirements is not actually a requirement?

Q10: Can you think any additional requirements besides these that recent EU regulations like AI Act, GDPR and DORA require?

Appendix B List of requirements

Table B.1: Requirements from the examined regulations

Requirement index	**Description**
GDPR.PR1	The data controller must provide certain required information to the data subject when requested
GDPR.PR2	The data controller must keep a record of processing activities
GDPR.PR3	Personal data must be either corrected or deleted when requested in applicable situations
GDPR.PR4	Personal data must be able to be left outside of processing when needed
GDPR.PR5	Data processing can have automated decision-making in it, but it has to be able to be removed from certain sets of data
GDPR.DR1	The development has to include a method to make sure, that all data handling processes in the developed program are logged and saved for possible lawful requests by data subjects

Continued on next page

Table B.1 – continued from previous page

Requirement index	**Description**
GDPR.DR2	The software development organisation has to have mechanism within it that review and change the development methods when they are detected not to be in accordance with regulations
GDPR.DR3	The used development methods must be adapted to have data protection by design in it from the start
GDPR.DR4	When developing software to be used in data processing, the used techniques and technologies should be as state-of-the-art as is appropriate considering the scope and nature of the data processing
GDPR.DR5	The development organization should have a structure within it that makes sure, that request from authorities are acted upon
GDPR.DR6	During development data use cases should be considered early so that the risks can be recognised, and those risks could be addressed
AI.PR1	High-risk AI systems have to include a Risk Management System
AI.PR2	High-risk AI systems that use AI models have to have data governance and management practices
AI.PR3	Technical documentation must be created for high-risk AI systems, and it has to be kept up-to-date

Continued on next page

Table B.1 – continued from previous page

Requirement index	Description
AI.PR4	The AI system must have instructions with it that include the characteristics, capabilities and limitations of performance of the high-risk AI system
AI.PR5	The high-risk AI system must have appropriate human-machine interface tools so that the risks of the system can be mitigated and recognised as much as possible
AI.PR6	AI systems must have instructions of use with them and those instructions must state the levels of accuracy of the system and the relevant accuracy metrics
AI.PR7	High-risk AI systems must be developed in such a way, that they are as resilient and robust as possible to withstand internal faults and external cybersecurity threats
AI.PR8	High-risk AI systems must have a Quality Management System
AI.PR9	Provider of a high-risk AI system has to keep technical documentation; documentation on the QMS; documentation of the changes; documentation of decision of notified bodies and EU certificate of conformity for at least 10 years from the moment when the AI system was placed on the market
AI.PR10	Automated logs of a high-risk AI system need to be kept for a period appropriate to the intended purpose of the high-risk AI system that is at least six months

Continued on next page

Table B.1 – continued from previous page

Requirement index	**Description**
AI.PR11	Provider of a high-risk AI system has to draw up an EU declaration of conformity for each AI system that they have
AI.PR12	All AI generated or manipulated content has to be marked as synthetically generated
AI.PR13	EU commission must be informed within two weeks after the system meets the requirements, or it becomes known that the system will meet the requirements for a high impact system
AI.PR14	Providers of general-purpose AI systems must draw up and keep up-to-date technical documentation of the AI system
AI.PR15	Providers of general-purpose AI systems must draw up and keep up-to-date documentation for providers who intend to integrate the general-purpose AI system into their own AI system
AI.PR16	Providers of general-purpose AI systems with systemic risk must try and mitigate those systemic risks by means of conducting model evaluations; maintaining an adequate level of cybersecurity; notifying and advising the AI Office of serious incidents and systemic risks at the EU level

Continued on next page

Table B.1 – continued from previous page

Requirement index	**Description**
AI.PR17	Providers of high-risk AI systems need to create a post-market monitoring plan and then follow it with the post-market monitoring system
AI.PR18	Providers of high-risk AI systems that aim to test their systems in real-world conditions must create a real-world testing plan
AI.DR1	The developer of an AI system must analyse the capabilities and use cases of the AI system throughout its development and life cycle
AI.DR2	High-risk AI systems have to be developed so that they can be overseen by humans efficiently throughout the period where the system is in use
AI.DR3	Developers of a high-risk AI system have to consider quality metrics like accuracy, robustness and resiliency throughout the development process and adapt the designs when required thresholds are not met
AI.DR4	Provider of a high-risk AI system has to keep vigilant watch over the system and take immediate action if the system is not in conformity with the AI Act. This action has to include measures to make the system conform to the AI Act again and also measures to notify all the required parties

Continued on next page

Table B.1 – continued from previous page

Requirement index	Description
AI.DR5	Provider of a high-risk AI system has to have at all times a clear picture of, is the system in conformity with the AI Act. Provider of the system has to also be able to prove it on request
AI.DR6	Providers of AI systems that generate content have to make sure that their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible
AI.DR7	Providers of AI systems must consistently measure and be aware of the AI system´s capabilities
AI.DR8	Provider of a general-purpose AI system must decide the tasks that the AI is fit to be used in and write those tasks down for the possible users and deployers of the AI system
AI.DR9	The provider of an AI system must carefully consider what they want to test and plan accordingly to ensure that the possible risks and adverse outcomes to the data subject are minimised
End of Table	