Software Development Compliance: Translating EU Cybersecurity Legislation into Practice for IoT and Embedded Systems

UNIVERSITY OF TURKU
Department of Computing
Master of Science (Tech) Thesis
Software Engineering
October 2025
Matias Suksi

UNIVERSITY OF TURKU
Department of Computing

MATIAS SUKSI: Software Development Compliance: Translating EU Cybersecurity Legislation into Practice for IoT and Embedded Systems

Master of Science (Tech) Thesis, 60 p., 3 app. p.
Software Engineering
October 2025

This thesis examines how the European Union's upcoming cybersecurity legislation will affect software in IoT and embedded devices. Motivation for the thesis has arisen from real-world Company X's preliminary investigation concerning the upcoming legislation that would have effect on the company's ventilation unit's control system. It translates legislation text into concrete engineering-level requirements that are needed for achieving compliance. The thesis maps relevant acts and outlines requirements that impose modifications to the software due to cybersecurity. Methodologically, the thesis is targeted literature and legal-text review which focuses on the practical implementation and conformity.

Findings indicate that three instruments concern software cybersecurity requirements: Radio Equipment Directive (RED) Article 3(3), Cyber Resilience Act (CRA) and Revised Product Liability Directive (RPLD). RED's new points can typically be met via self-assessment against harmonized standards (EN 18031 series) if scope and exceptions are correctly regarded. CRA introduces broad, risk-based obligations across the product life cycle. It covers essential security requirements, vulnerability handling, user information, technical documentation and vulnerability reporting. RPLD expands liability to digital products and software, indirectly raising the concerns for secure-by-design practices. In contrast, the Data Act mainly mandates data-access and sharing rights and process duties for connected products but does not prescribe concrete cybersecurity controls.

Across the acts, the biggest consequence for manufacturers is an increased documentation and conformity assessment workload, even where existing security practices are already strong. The thesis combines these obligations into practical guidance for embedded and IoT software products' manufacturers.

Keywords: IoT, embedded device, embedded system, cybersecurity compliance, RED Article 3(3), Cyber Resilience Act (CRA), Data Act, Revised Product Liability Directive (RPLD)

Contents

1 Introduction **1**

1.1 Background and motivation 1

1.2 Objective 2

1.3 Scope 3

1.4 Method 4

1.5 Structure 5

2 Cyber secure software **6**

2.1 Embedded system and IoT 6

2.1.1 Definitions 7

2.1.2 Relationship of two concepts 8

2.2 Basics of cyber secure software 8

2.2.1 CIA triad 9

2.2.2 SSDLC 10

2.3 Embedded and IoT systems' security 15

2.3.1 Threats and attacks 16

2.3.2 Vulnerabilities 18

2.3.3 Attack scenario diagram 19

3 Control system **20**

3.1 Structure of system 20

3.2 Motivation 20

4 Regulation of EU **22**

4.1 Legal instruments of EU 22

4.2 RED Article 3(3) 23

4.3 Data Act 25

4.4 CRA 26

4.5 RPLD 27

5 Requirements of acts **29**

5.1 RED Article 3(3) 29

5.1.1 Harmonized standards 29

5.2 Data Act 41

5.2.1 Definitions 41

5.2.2 Requirements 42

5.2.3 Compliance 45

5.3 CRA 46

5.3.1 Requirements 46

5.3.2 Compliance 51

5.4 RPLD 51

5.4.1 Compliance 51

6 Consequences for IoT and embedded devices **53**

6.1 RED Article 3(3) 54

6.2 Data Act 54

6.3 CRA 55

6.4 RPLD 56

6.5 Additional takeaways 56

7 Conclusion **58**

7.1 RQ 1 58

7.2 RQ 2 59

7.3 Restrictions 60

References **61**

Appendices

A Summary of EN 18031-1:2024 (1/2) **A-1**

B Summary of EN 18031-1:2024 (2/2) **B-1**

C Summary of EN 18031-2:2024 **C-1**

1 Introduction

Policy and law makers of EU have started to adopt measures for mitigating consequences of cybersecurity incidents and preventing them. EU defines cyber resilience one of the key policies and as concepts where organizations should be prepared for cyber attacks and have ability to recover from them. [1]

This cyber resilience is a key theme in this thesis, where we discuss how the upcoming cybersecurity acts of EU are affecting the IoT and embedded device's software. We start with motivation of this thesis.

1.1 Background and motivation

A motivation for this thesis arose from real-world stress and challenges of "Company X" considering upcoming EU cybersecurity acts. Company X, as we call it throughout the thesis, is one of the market leaders of the ventilation solutions and products in Finland. They offer different kinds of ventilation-related products such as ventilation units, roof-installed extractors, cooker hoods, filters and fans.

Considering the background for this thesis, Company X has already observed that new cybersecurity acts are presented almost every year, or at least rough skeletons of them, by EU. Company X has observed that many acts are, especially concerning the cybersecurity of manufactured products. Company X had requested consultation already from lawyers and consultants in the field considering upcoming acts, but even the professionals in the field have not been able to produce a clear overview or plan of how the company should

cope with these new acts. They could not provide clear answers without hesitation regarding questions such as:

- Which acts will concern our products?
- If an act concerns our products, what are necessary concrete modifications to our software products for achieving sufficient compliance?

1.2 Objective

This thesis's research objective forms from previously mentioned real-world questions, and it discusses converting legislation text into practice. The main goal of this thesis is to provide summary of concrete actions which are necessary for fulfilling the requirements of upcoming acts considering the IoT and embedded devices' software.

Before it is possible to provide concrete summary of actions, a comprehensive overview of the upcoming acts is done. This overview includes defining and interpreting the acts, determining which are concerning IoT and embedded devices' software and in which time they become in force. The acts which are in their planning phases and will be presumable concerning IoT and embedded devices will also be mapped out. The control system of Company X's ventilation units can be seen to represent quite common IoT product. The ventilation unit has a resource-limited computer inside, which powers three different types of user interfaces that are accessible for end-users.

Investigated acts are chosen based on the preliminary investigation of Company X which will very likely to affect their ventilation units' control system. Based on this, the objective of this thesis is to provide generalization on how the upcoming EU acts can affect overall embedded and IoT systems and provide general guidance for private companies for achieving required compliance. It must be already noted that strict punctual generalization can not be concluded since the actions needed will be dependent on the

requirements of the field of products. It is self-evident that medical embedded devices might have to fulfill much stricter acts than just a ventilation unit.

The research questions of this thesis are as follows:

- RQ1: Which acts have an effect on IoT and embedded devices' software's cybersecurity?
- RQ2: What are the consequences of the new upcoming acts for the devices' software and the manufacturers of these devices?

1.3 Scope

This thesis includes only acts presumable concerning the customer-deliverable software product of the ventilation units and its development life cycle, which is the control system of the ventilation unit. Company X does not offer any other significant customer-deliverable software products, so research is done based on this control system.

The thesis not only lists the technical requirements of the software, but also, for instance, the requirements set for software product manufacturers regarding software development processes and documentation. A main focus of this research is on the actual cybersecurity acts, but it must be noted that there are acts which are heavily related to the cybersecurity without being actual cybersecurity acts. These direct and indirect cybersecurity acts are defined for this thesis as follows. Direct acts concern cybersecurity distinctly. Indirect cybersecurity acts are defined as heavily tied acts with cybersecurity, but do not explicitly express requirements considering cybersecurity.

The research excludes the acts which are not trivially concerning the control system, such as Digital Operational Resilience Act (DORA) [2] since it is clearly expressed that it is concerning only a financial sector. Also, acts which are already in force, or will be in force during the start of this research, are excluded since these are already investigated by the company, listed as an example NIS2 [3].

Since the main goal is to turn legislation into practice, the main focus of the thesis is to list requirements and concrete consequences of upcoming acts. For instance, the thesis just touches the rationale behind the acts, and it does not map what sanctions are issued if the manufacturers do not achieve compliance with their products.

1.4 Method

Reviewing literature in this thesis concentrates heavily on the upcoming acts, but also fundamentals of implementing cyber secure software. Some relevant topics are excluded from the literature review, since they are already heavily researched topics and due to this they are referenced directly throughout the thesis, for example GDPR.

The search expression used for finding research papers about the acts is as follows:

- ("IoT" OR "embedded device" OR "embedded system") AND ("<placeholder for act's name>") AND ("software") AND ("in practice" OR "compliance")

The aim of the search expression is to limit found research papers so that only relevant papers are found considering practical software implementation and achieving compliance of acts. Since this is also the main goal of the thesis, it is not interesting to review direct legislation text of EU, but in utilizing the existing, already completed research about the practical aspect. However, it must be noted that since these upcoming acts are recent topics and constantly evolving, there is not much relevant peer-reviewed research material available yet, or they are already become outdated, which in some places forces this thesis to rely on the legislation text of EU. Several supplementary search expressions are also used, the purpose of which is to gather supportive material and basic theory which are underlying below these upcoming acts.

Since the scarcity of relevant peer-reviewed material, searches were sorted relevancy-first. In some places too old articles were excluded, since proposals and acts' specifications are constantly changing. There was no possibility for systematic exclusions, since

currentness of each act forced to use own consideration with each topic. Some articles were outdated even though they were released last year, but some articles were valid even from 2018. Information was searched from Google Scholar, ACM Digital Library, IEEE Explore and ScienceDirect but also supervisory authorities of the acts such as from Traficom and also directly from European Commission.

1.5 Structure

Next, a structure of the thesis is described. Section 3 describes the control system of the ventilation unit in brief. This is essential for understanding the initial perspective from which this research is conducted. Sections 2 and 4 form a literature review of this research. Section 2 discusses general topics concerning secure software, how secure software should be implemented, and definitions of important matters that are necessary for comprehending the subject of the thesis, such as definitions of embedded devices and SDLC. Section 4 digs into the main subject, which is the EU's upcoming cybersecurity acts. In this section, the acts are presented, how they are enforced and what cybersecurity aspects they cover. Section 5 covers the acts in more detail, and in this section the main goal is to gather concrete requirements of the acts. This act listing is utilized in the Section 6, which summarizes the practical implications for IoT and embedded devices' manufacturers and for their software based on the found requirements. Finally, we present answers for the research questions.

2 Cyber secure software

Software developers often overlook the security of software, and it can often remain as an afterthought. They rely on their intuition and own feelings rather than following common guidelines even though there are numerous practical frameworks available for developers and organizations. These frameworks and practices constantly change with evolving cyber threats and regulative landscape. [4][5]

To understand basic methodology of this research, we discuss how secure software should be implemented and what general practices are there for secure software development. A big emphasis is especially on security topics with embedded devices, and which threats embedded systems are facing and how these practices aim to tackle the threats. These topics are crucial for understanding the background of acts concerning the cybersecurity of software and later these practices are utilized in practice for achieving compliance with upcoming EU legislation.

2.1 Embedded system and IoT

The topic of this thesis mainly focuses on how upcoming legislation affect specially embedded systems and IoT. These two terms get mixed quite often and they are used to describe the same thing, even though it is not true. They have similarities and relationships between each other which can cause confusion. [6] There is clear need to distinguish these two terms.

2.1.1 Definitions

Embedded system is a computing system which is designed for a specific function. Embedded systems can be independent devices or be a part of larger system. They are developed for particular purpose to meet real-world constraints, such as low power consumption or low cost, in contrast to general-purpose computers such as PCs. [7] Embedded systems can be classified depending on their performance and functional requirements, depending on the performance of microcontrollers and based on their deterministic behavior [8]. Examples of embedded systems are TVs, washing machines, automobiles and smartwatches [7]. *Cyber-physical system* is another name for embedded system. The term was created based on the nature of embedded systems that they often combine the intelligence of computers with physical objects of the real world [9].

IoT (Internet of Things) device refers to device which includes sensors, software and other technologies to connect and exchange data with other devices and systems over the internet or other communication networks [10].

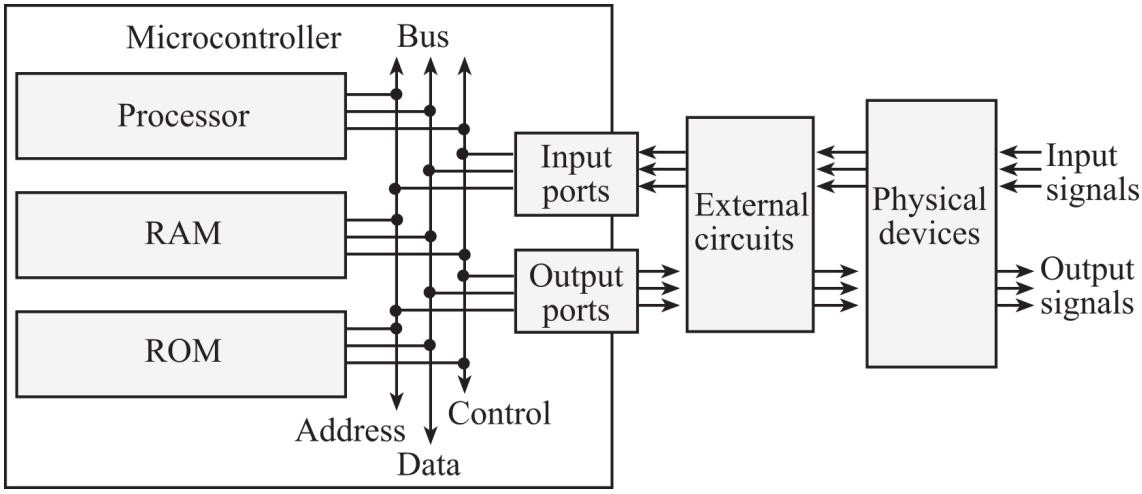

Figure 2.1: Block structure diagram of embedded system [7][11]

Figure 2.2 demonstrates structure of common embedded system. The embedded system includes a microcomputer which interacts with external physical devices. *Microcontrollers* are complete computers as a single package where processor, RAM, ROM and I/O

ports are included. These are often utilized in construction of embedded systems since they have low cost, compact size and low power usage. [9]

2.1.2 Relationship of two concepts

All IoT devices are embedded devices, but not all embedded devices are IoT devices. The relation between these two depends heavily on connectivity. By IoT device's definition, it requires that device possesses some kind of networking interface which enables it to communicate with other devices. Usually this network is internet, as its name states, but the network can mean network which is something else than internet. However, there are also embedded devices which are not connected to network whereupon they are not considered as IoT devices. [6] This can be demonstrated easily with the real-world case of this thesis.

Company X's ventilation units are not, by default, communicating within any kind of network. In this case, ventilation unit is not considered as IoT device since it is not communicating with external world, even though it has capabilities to do so. However, users have an option to connect their device to the internet and to the cloud, if they want. In this case, ventilation unit becomes IoT device. However, all this time, ventilation unit has been embedded device.

Due to the definitions, observations and conclusions made in this thesis for IoT, it is also set to apply to embedded systems. Also, this goes partially for vice versa, when considering the connectivity requirement of IoT.

2.2 Basics of cyber secure software

Cybersecure software forms from obeying guidelines, best practices and knowledge. Implementing cyber secure software is one of the most important issues and biggest challenges for companies in their software development life cycles (SDLC) and achieving

regulatory requirements and standards. [12]

2.2.1 CIA triad

Considering the fundamentals of achieving security in computer systems, there is a concept called CIA triad. CIA triad forms from three fundamental dimensions which are defined as follows. [13]

- **Confidentiality:** Ensuring that an asset is accessible only to authorized facets.
- **Integrity:** Preventing unauthorized modifications, corruption or destruction of the asset. A system performs its intended function without impairing it.
- **Availability:** An asset is available for authorized facets promptly.

Figure 2.2: CIA triad with their opposites [14]

These fundamentals of software security are a motivation for different kinds of security mechanisms such as authentication and authorization. [13] CIA triad is a key concept of security since its dimensions appear constantly in the relevant literature, whether it is about quality attributes of software or overall security principles. Systematic literature review of Hernan Nina, José Antonio Pow-Sang and Mónica Villavicencio about secure software development [15] lists these CIA triads dimensions as the most frequently appearing security principles in their conducted mapping.

2.2.2 SSDLC

Secure Software Development Life Cycle (SSDLC) is a framework whose goal is to address the importance of minimizing security risks at every stage of SDLC. This framework is an essential response to the issue that the security of software should not be an afterthought. SSDLC consists of the same phases as SDLC, but it includes in each phase additional security measures for software. [5] There are no strict definitions for SSDLC and SDLC. Multiple definitions are present but all these definitions share the same main idea. Next, a general structure for SSDLC is described. Venkat Boppana defines in the article [5] SSDLC with the following phases.

Planning and requirements definition

Defining security requirements: Defining requirements for functional and security aspects of software with stakeholders. *Threat modeling:* Identifying possible attack vectors and mapping how attackers can exploit the system. *Risk analysis:* Identifying risks and an impact on the system if an exploitation happens. [5]

Designing

Secure architecture: Creating the system's architecture while keeping in mind the security considerations. *Security protocols:* Obeying found to be safe security protocols. *Secure design principles:* Obeying secure design principles such as Least Privilege, Separation of Duties, and Fail-Secure Defaults. [5]

Development

Secure coding standards: standards give common guidelines on how safe code should be implemented which helps to maintain consistency and minimizes chances of leaving vulnerabilities in software. *Defensive programming:* Coding in a way that prepares for possible attacks and errors. *Using safe libraries:* Using safe and maintained libraries

with strong security. *Avoiding common vulnerabilities:* Developers should be aware of common vulnerabilities such as cross-site scripting (XSS), buffer overflows, and SQL injection and avoid these by obeying safe coding practices. [5]

Testing

Employing security testing methodologies: There are methodologies for inspecting software such as Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). *Penetration testing:* Emulating real-world attacks against the system to find vulnerabilities. *Vulnerability scanning:* There are automated tools that can be utilized for identifying security issues in the system. [5]

Deployment and post-deployment

Secure deployment practices: The environment of the system should be configured properly when deployed. Firewalls should be enabled and set up correctly and databases or servers should be secured. *Continuous monitoring:* Monitoring system for security threats while it is in production. This includes logging and analyzing events of the system and tracking unusual behavior within it. Intrusion Detection Systems (IDS) can be used for alerting if exploitation happens. *Incident response:* It is a fact that incidents still happen even if the best security practices are followed. There should be documented and practiced response plans if an incident occurs within the system. This enables quick response from the administrative facet and helps to minimize possible damage. *Patch management:* New vulnerabilities occur and they should be fixed. Patch management includes tracking known vulnerabilities, updating components of software, and ensuring that patches are deployed to production in time. [5]

There are different kinds of implementations and emphasis on how this framework is employed in practice. Systematic Mapping of the Literature on Secure Software Development [15] lists common Secure Software Development Models (SSDM) in their

systematic literature review which appear most in their mapped articles. In some articles, these are called Secure Coding Standards (SDS).

N°	Secure Software Development Model	Percentage
1	OWASP - Comprehensive Lightweight Application Security Process (CLASP)	41%
2	MS Microsoft - Microsoft Security Development Lifecycle (SDL)	27%
3	NIST	11%
4	Gary MG - McGraw's Touchpoints	11%
5	ISO/IEC (such as 13335, 13849, 21434, 26262, 27002, or 27034)	9%

Table 2.1: Secure Software Development Models
[15]

These SSDMs appear most in the mapping of Hernan Nina, José Antonio Pow-Sang and Mónica Villavicencio [15] but it does not necessarily mean these are always the most used ones. There are popular models such as Security Apple Developer, Web Application Security Consortium (WASC), and SANS information security training which do not appear in the studies [15]. Next, the most common SSDMs are discussed in more detail.

OWASP - CLASP

OWASP's Comprehensive, Lightweight Application Security Process (CLASP) is the light process for developing secure software. It is constructed of 24 top-level activities that can be customized based on the needs of the development process. It has several key points which are:

Main objective security: The most important objective for CLASP is to enable the building of software where security is a number one priority. CLAPS has a theoretical perspective on this security topic and the activities that CLASP includes are quite extensive.

Limited structure: CLASP is a set of independent activities that need to be integrated into the development process and its operating environment. CLASP enhances flexibility and the choice of which activities should be included in the development process, and which orders are left open.

Roles: CLASP introduces roles that are used as perspectives to structure security activities. Roles are essential for ensuring the finish and quality of activities' outcomes.

Lot of supporting resources: CLASP has a broad range of security resources that can be used as guidance for implementing activities. One example of this kind of resource is a list called "104 know security vulnerabilities in application source code". This list can be used as a checklist during code reviews. [16]

McGraw's touchpoints

McGraw emphasizes 7 touchpoints that should be considered in phases of SSDLC [13]. These touchpoints are mapped with development phases as follows:

- **Abuse cases - requirements:** Defining behavior for the system that should be achieved under different kinds of abuses
- **Security requirements - requirements:** Defining security requirements
- **Architectural risk analysis - design:** Considering security during design
- **Risk-based security tests - test planning:** Testing security functionality with a standardized methods
- **Code review and repair - coding:** Eliminating problems
- **Penetration testing - testing and deployment:** Identifying relevant problems
- **Security operations - deployment:** Taking care of security in production

[13]

As seen, McGraw's touchpoints fit seamlessly inside the general definition of [5] since the touchpoints emphasize aspects that are already very similarly included inside the general definition even though there are additional more detailed touchpoints such as including abusing cases in requirements definition.

Microsoft's SDL

In 2002, Microsoft mapped the most frequently occurring security issues in their products and based on this mapping a new SDL called Microsoft SDL was born. It forms from activities that were initially developed to support overall Microsoft's development process and particularly paying attention to security issues. Microsoft SDL has these kinds of characteristics:

Security as supporting quality: SDL aims to increase the quality of functionality-driven software by enhancing its security and it sees that its security activities are additional add-ons to the already existing software construction process, nor as separate cybersecurity part.

Well-defined process: SDL is organized, and activities are grouped in stages. Stages concentrate heavily on security topics. They are easy to integrate into standard software development phases. SDL highlights that some activities have a continuous nature in the process, such as threat modeling and education. These activities should always be carried out continuously to improve results.

Good guidance: SDL gives good guidance on how activities must be executed even though they are sometimes concrete, and sometimes more pragmatic. Due to this guidance, completing an activity in SDL is easy even for less experienced developers. [16]

NIST

The National Institute of Standards and Technology (NIST) is a department of the US government. NIST provides guidance, regulations, and rules on how software should be developed and security ensured. It offers tons of free guideline documents that should be used for integrated control systems (ICS) including supervisory control and data acquisition (SCADA), distributed control systems (DCS), and for many other industry fields. These documents include best practices on how these systems should be secured. They bring out known threats, review architectures of systems, and offer countermeasures to

respond correctly to these threats. [12]

ISO/IEC

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are committees that are maintaining, developing, and creating standards in manufacturing, heavily focusing on ICT technologies and also electric and electronics. Some of the standards are available for free, some are chargeable. [12] There are lot of different standards that are related to the cybersecurity of software where the systematic mapping [15] lists as an example ISO 13335, 13849, 21434, 26262, 27002 and 27034.

2.3 Embedded and IoT systems' security

Next, SSDLC is presented, and attention is turned specifically into embedded systems' software and how it should be secured. Embedded systems share same security concerns as general-purpose computers. However, the main problem is that embedded systems have additional design constraints which makes some well-known vulnerabilities of the general-purpose computers more dangerous or easier to exploit in constrained embedded systems. [17]

In conducted literature scanning of this thesis, it is quickly noticed that the articles which refer to securing specifically embedded or IoT systems, importance of same common SSDLC is highlighted which applies for all software in general. There is lot of discussion which implicitly refers to general SSDLC without distinct reasoning. However, what makes the difference is that in the articles which consider in more detail the threats faced by embedded and IoT systems, based on these threats the application of SSDLC is discussed. Because of these observations, it is focused on common threats and vulnerabilities of embedded and IoT systems.

2.3.1 Threats and attacks

A threat is any potential danger for exploiting vulnerability to cause harm or damage to a system [18]. Anthony Dessiatnikoff [17] presents three main classes for software-oriented attacks in the article concerning vulnerabilities especially in avionic embedded systems. These attack classes are attacks against core functionalities, attacks on fault-tolerance mechanisms and attacks on firmware updates where the attacks against core functionalities are considered the most important one. The author considers attacks on firmware updates as an additional class. Attacks on fault-tolerance mechanisms concern more safety-critical embedded systems so it is not considered as important class for this work, since we are looking for generalization for embedded systems in general. The author sees that general-purpose computers have resemblances with embedded systems and the attacks against core functionalities are derived from this view. These are considered the most important threats for this work.

Attacks against core functionalities

There are multiple subclasses for attack against core functionalities.

Attacks on processor: Modern processors have sophisticated features for improving their performance. Modern processors have often multiple cores, cache with multiple layers, memory management unit (MMU) or branch predictor. The downside of these features is that they can introduce security issues. It is investigated that it is possible to acquire cryptographic keys from caches or by exploiting branch predictors' prediction mechanisms. Denial of Service (DoS) attacks are possible to conduct by crashing the processor with feeding undefined or undocumented instructions into it. This can lead to situations where the processor proceeds to service mode which could be even more beneficial and stimulates more rights for attackers. [17]

Attacks on memory management: Memory is a wide concept since it can mean random access memory (RAM) but also runtime environment of processors such as regis-

ters, or input/output (I/O) devices' memory. These kinds of attacks exploit vulnerabilities in memory management in software, and they can exploit also I/O mechanisms to gain direct memory access (DMA). Memory access attacks can have different targets and to distinguish these targets, memory management attacks can be categorized into application, operating system (OS), hypervisor and CPU environment attacks. [17]

The most straightforward way to access memory is to utilize the processor of system. Buffer overflows or badly formatted string inputs can be utilized for gaining unauthorized memory access. The most dangerous memory attack is a kernel attack where vulnerability is not located on application level but in the kernel of the operating system. This enables attackers to execute malicious code directly with the kernel's permission. [17]

Attacks on communications: Dessiatnikoff discusses in more detail communication protocols which are more common in avionic systems, such as AFDX networks. These topics are ignored. However, he emphasizes several points which are relevant for embedded systems in general.

Communication includes all kinds of information exchange between two or more entities. Communication can be communication between processes, which is implemented for example with IPC (Inter Process Communication), or it can be data exchange between machines or modules via communication buses, such as Ethernet. Typical attacks against communication channels are data tampering or man-in-the-middle (MitM) attacks. [17]

Attacks on time management: Embedded systems often include different clocks or interval timers for timing processes, such as Real Time Clock (RTC), Programmable Interval Timer (PIT), Time Stamp Counters (TSC) and High Precision Event Timer (HPET) which are crucial for the operation of the system. Attackers can tamper these clocks, for example, by modifying their configuration registers and generating false stop conditions. [17]

Attacks on process management: Execution of processes is controlled by scheduler which determines how long processors should execute certain process and when. When a

reserved time slot for the process is finished, scheduler moves the execution for the next process in line. Attackers can exploit flaws in scheduler's operation which can cause a situation where system does not meet anymore requirements of the real-time system. [17]

Attack on cryptographic mechanisms: Cryptographic mechanisms can have vulnerabilities. Flaws can be detected years after development work and increased computation power can make them unusable. Even though commonly used cryptographic algorithms are found proof, they can be exploited by acquiring their cryptographic keys with utilizing flaws in other parts in the system, for instance in memory management. [17]

Attack on ancillary functions: Ancillary functions are features which purpose is to support operation of processors. These functions can be related to power management, overclocking or temperature control. For instance, Intel's processors SMM (System Management Mode) can be exploited for gaining access to whole memory space. [17]

2.3.2 Vulnerabilities

A vulnerability is a flaw or a weakness in a system protection that can be exploited [18]. Dorottya Papp, Zhendong Ma and Levente Buttyan [19] investigated Common Vulnerabilities and Exposures (CVE) database for mapping out vulnerability types of embedded systems. The classification of vulnerabilities is based on their findings.

Many vulnerabilities are born from programming errors which can expose different kinds of control flow attacks. For instance, input parsing vulnerabilities can lead to buffer overflows issues. Often embedded systems have a web-based interface for configuring and updating the system. It is typical that these kinds of devices are rarely updated which introduce security risks. There are risks concerning weak access control and authentication. Many devices are left on with default or weak passwords, or they include hard-coded passwords which offer a possible backdoor access for people who know the password. It requires minimal effort to bypass the access control mechanisms if such vulnerabilities exist. Improper use of cryptographic can lead to fatal security failures when they are

not used properly, such as utilizing weak random number generators for cryptographic key generation. [19] It is also important to note that there exist unknown vulnerabilities. Dorottya Papp, Zhendong Ma and Levente Buttyan observe that there exist unknown vulnerabilities which targets, and the effect of attack are known but the exploited vulnerability is unknown.

2.3.3 Attack scenario diagram

The basic terms of software security for embedded systems are unwrapped. Now, it is place for the demonstration of their relations.

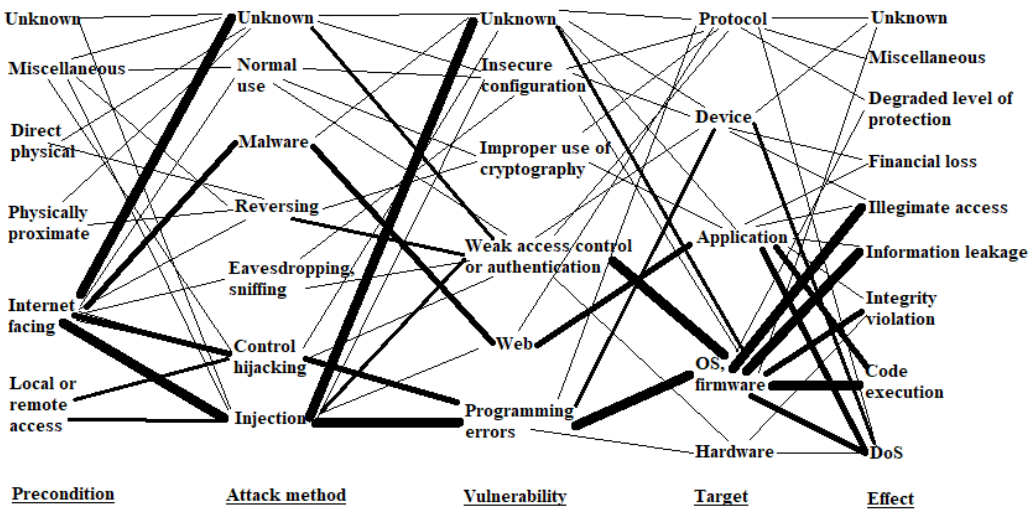

Figure 2.3: Common attack scenarios [19]

Figure 2.3 demonstrates different attack scenarios. The thickness of each path between the dimensions describes how often CVE entries noted this path as realized and involved path for the attack scenario [19]. The main take away from Figure 2.3 is that even though it points out paths which are clearly the most probable paths to conduct certain types of attacks, there are still multiple alternative routes for conducting similar attacks. This reflects the complexity of implementing secure software in embedded systems.

3 Control system

Next, a more comprehensive description of Company X's ventilation units' control system is provided. The description remains still rather superficial to protect trade secrets of the company.

3.1 Structure of system

Figure 3.1 is a complete outline of the control system. The figure describes all components, interfaces and main technologies which are part of the ventilation unit. Some of the components are more relevant than others. Some are considered optional accessories, and some are compulsory parts of the control system which are essential for controlling the ventilation unit.

3.2 Motivation

The main idea why we illustrate the control system is to give some motivation to explain why certain legislative acts are excluded from this work. Chosen acts in this thesis are chosen based on the preliminary investigation of Company X. According to this preliminary investigation, these chosen acts for this work are Cyber Resilience Act (CRA), Radio Equipment Directive's (RED) new points, the Data Act and Revised Product Liability Directive (RPLD). For instance, DORA and the Cyber Solidarity Act (CSA) are excluded from this work because they specifically apply to companies operating in the financial or

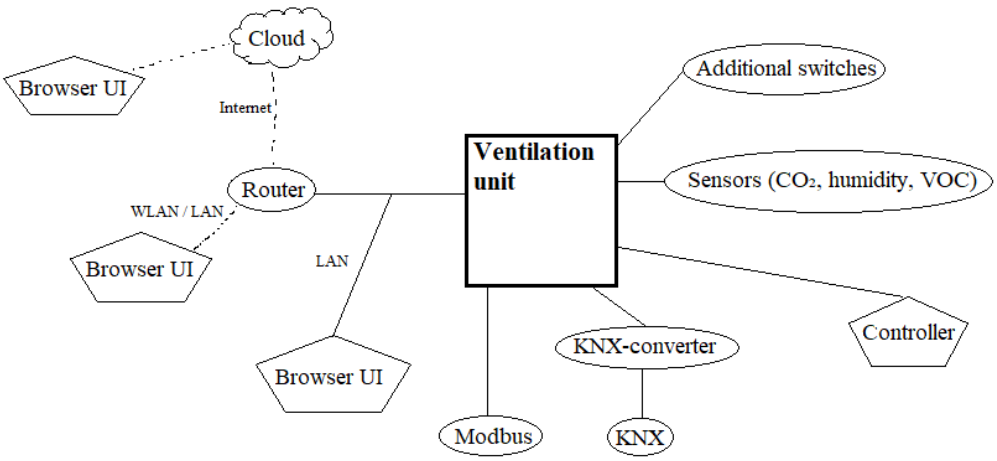

Figure 3.1: The control system of the ventilation unit

critical infrastructure sectors. Company X does not utilize Artificial Intelligence (AI) in its software development, at least yet, so AI Act is excluded from this work.

However, acts which are very presumably concerning ventilation unit's control system and could presumably introduce cybersecurity requirements are covered. Since investigation is started from scratch, there is possibility that in this thesis presumably relevant acts are covered and eventually it turns out that they are insignificant for this work.

4 Regulation of EU

In past two decades EU's cybersecurity policy has changed tremendously, and it is now one of the most important security policies of EU. EU is conscious about its increased reliance of digital infrastructure and services, and how certain sectors are depended on safe use of ICT (Information and Communication Technology) infrastructure. [20]

Considering IoT security, it has very few designated standards or regulations compared to other technical solutions [21]. Next, we deepen into EU's cybersecurity policy and regulative landscape.

4.1 Legal instruments of EU

Here, the most important legal instruments of EU are presented and their differences explained. These instruments are easily confused with each other, and it is certainly necessary to clarify them.

Act is broad term for different legal instruments of EU. There are five main types of acts which are regulation, directive, decision, recommendation and opinion. Acts can be legislative or non-legislative. Legislative acts are adopted via co-decision or legislative procedure involving the Council and European Parliament. Non-legislative acts are adopted by the European Commission to implement legislative acts. [22]

Directive is legislative act that sets out a goal which all EU countries must achieve. However, even though the goal is common for all, it leaves it up to individual countries to decide how the goal should be achieved through their own national laws. [23]

Regulation is one type of legislative act. A regulation has general application, and it is directly applicable in EU Member States without national implementation. [24]

Standard is voluntary technical specification. Harmonized standards provide presumption of conformity for companies that their products comply with EU laws. [25]

4.2 RED Article 3(3)

Radio Equipment Directive (RED) is an EU directive which sets requirements for devices which operate with radio frequencies. RED concerns almost all radio devices placed on the EU market with certain exceptions. The directive does not concern radio equipment used in national security, defense, public safety, aviation and maritime safety. Amateur radio equipment and devices used only in R & D are also excluded from the sphere of influence of the directive. [26] These are the summarized exclusions.

RED consists of many different articles but the most interesting for this research is Article 3 which lists essential requirements for radio equipment placed on EU market. More precisely, the most interesting points are in Article 3(3) due to their relevance for cybersecurity topic and currentness. Article 3(1) declares requirements considering user healthy and safety but also considering EMC. Article 3(2) enhances the importance of efficient use of radio spectrum. This includes that radio equipment must not cause harmful interference. Article 3(3) lists additional essential requirements for certain radio equipment on top of Articles 3(1) and 3(2). The points (d, e, f) of Article 3(3) set requirements considering cybersecurity, privacy and fraud protection. [26] These points became in force 1.2.2022 and are applied from 1.8.2025 [27]. The points are applied without national implementation [28]. As stated, Article 3(3) concerns only certain radio devices. The cybersecurity requirements of RED are considering radio devices which are such as internet-connectable (WLAN access points, smartphones), toys, childcare devices and devices which are wearable on human body (smartwatches) [27]. The new points are

declared in the directive as follows:

- **Article 3(3) (d):** "Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service" [26].
- **Article 3(3) (e):** "Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected" [26].
- **Article 3(3) (f):** "Radio equipment supports certain features ensuring protection from fraud" [26].

The cybersecurity requirements of RED are defined in EN 18031:2024 standard. The reviewing of compliance of radio devices with RED's cybersecurity requirements can be done with two ways. By obeying a harmonized standard, a manufacturer of radio device can show fulfilling of requirements by itself. Another option is with the help of the notified body if harmonized standards are not obeyed for some reason. There are also special cases where the notified body must perform assessment and self-assessment is not allowed. [27] There are certain exceptions where harmonized standards do not guarantee compliance. The exceptions are listed as follows:

- **Restriction 1:** Sections "rationale" and "guidance" in harmonized standards EN 18031-1:2024, EN 18031-2:2024 and EN 18031-3:2024 do not guarantee compliance of Article 3(3) points (d, e, f).
- **Restriction 2:** The harmonized standards do not guarantee compliance of Article 3(3) points (d, e, f) if user can not set or use any password.
- **Restriction 3:** The harmonized standard EN 18031-2:2024 does not guarantee compliance of Article 3(3) point (e) if radio device does not implement parental or guardian access control.

- **Restriction 4:** The assessment criteria for secure updates of harmonized standard EN 18031-3:2024 does not guarantee compliance of Article 3(3) point (f) if it is about treating financial assets.

[29]

European Commission does not provide guidance how the harmonized standards should be applied to products rather this remains a responsibility of the manufacturer [29].

4.3 Data Act

Data Act is a new EU act that came into force on 11.1.2024 and it is generally applied from 12.9.2025. The motivation for implementing The Data Act arises from the reluctance of voluntary data sharing and its main goal is to strengthen mandatory data sharing between stakeholders in non-commercial and commercial data systems. [30] The Data Act aims to enhance fair, competitive and innovative data economy by regulating access and use of non-personal data and it is particularly concerning IoT devices. Data sharing rules are established for the users, third parties and public bodies. [31]

IoT devices store a lot of data, but manufacturers rarely provide access for users of the device even though the users are often the carriers of the physical devices which are collecting and storing the data [32]. Considering the Data Act with IoT devices, the Data Act aims to provide rights for users of IoT devices to access data via law and obligations addressed to manufacturers of products. This means that upon request, users can get access to the collected data which is generated by the use of the device or give this data to third parties. There are also special situations where access can be granted to authorities. It must be noted that this does not provide access upon request for other facets such as public or other market actors. [30][32]

GDPR is fully applicable to activities which are concerning personal data under the Data Act. The Data Act does not regulate the protection of this data. It must be noted

that the Data Act complements and specifies GDPR in some cases, but in the case of a conflict, GDPR overrides the Data Act with its protection of personal data. [33]

4.4 CRA

Cyber Resilience Act (CRA) is an act of EU which introduces common mandatory cybersecurity requirements for products with digital elements. This includes both hardware and software throughout their entire life cycle. It aims to ensure cybersecurity of digital products placed on the EU market and harmonize requirements across Member States. Also, it aims to enhance awareness of users about cybersecurity matters and to make cybersecurity recognizable metric which users can assess when using product or making purchase decision. [34]

CRA applies to the products with digital elements, and which can connect directly or indirectly to another device or network. The product with digital elements in the context of CRA is defined as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately"[35]. The broad definition contains naturally vast range of products which fall under the act. This includes e.g. consumer electronics, business software and industrial control systems. Products already covered by specific EU cybersecurity laws are excluded, listed as examples of medical devices and aviation software. [36]

CRA has already been in force since 10 December 2024 but its obligations and requirements are not applied yet [36]. Figure 4.1 reflects the timeline of applying CRA's obligations and requirements.

First applied obligations are concerning the provisions on notification of conformity assessment bodies. These obligations will be in force from 11 June 2026. From 11 September 2026, reporting obligations considering actively exploited vulnerabilities and severe incidents impacting on the security of products with digital elements are applied.

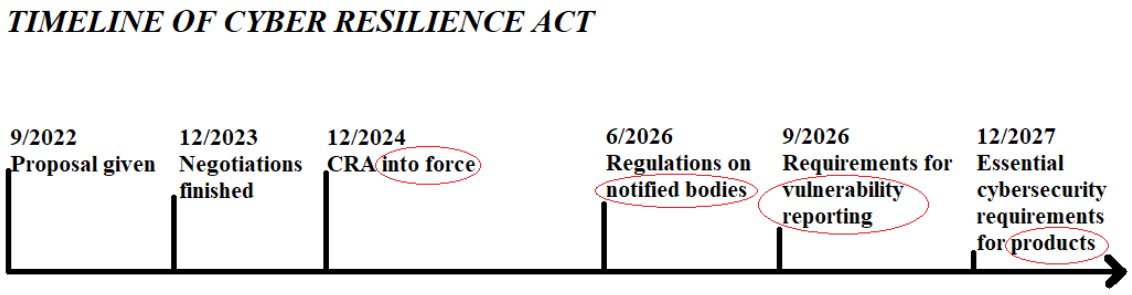

Figure 4.1: Timeline of applying CRA [37]

Lastly, from 11 December 2027 products placed on EU market must comply with essential cybersecurity requirements set in the act. [36] The obligations and requirements of the act are discussed more deeply later.

4.5 RPLD

In 1985, EU introduced *Product Liability Directive* (PLD) which set up that companies can be held liable for harm caused by "products". The "product" was defined explicitly as all movable objects with few exceptions. Even though the definition is already broad, it has not been able to keep up with technological advancements. [38]

The new *Revised Product Liability Directive* (RPLD) was adopted from 30 May 2024 and will be eventually applied from 9 December 2026 which expands this liability in terms of its scope and defendants. RPLD expands its previous scope to include more types of products. RPLD includes now also digital solutions. [39] Now companies can be held liable e.g. digital products, software, AI solutions, updates and smart devices defects. Also, scope of responsibilities is expanded. Previously, only manufacturers were responsible for defects. According to the new RPLD, also importers, distributors and platforms can be defendants. [39]

Standard of the defect is revised in RPLD. Previously, fair compensation could be claimed if the products fail to ensure safety, which should be entitled to expect or is

required. In RPLD this remains mostly same, but it clarifies that product is not considered defective just because there is better alternative product placed on market. [39]

5 Requirements of acts

In this section, we analyze how compliance of the acts can be achieved, and we discuss RQ1. First, the concrete requirements are gathered and based on the gathered requirements, the compliance actions are defined. It is important to remember that the analysis here has been conducted based on the information that is currently available about the topic while doing this research. In the literature review, we observed that due to the currentness of the topic, new information is emerging constantly. The chosen acts for the analysis are chosen based on the preliminary investigation, which was conducted in Section 4, where presumably concerning acts are taken into account.

5.1 RED Article 3(3)

RED is categorized in this thesis as a direct cybersecurity act since it was not cybersecurity act itself but after its recent updates it addresses now also cybersecurity requirements for radio devices' software.

5.1.1 Harmonized standards

As recently presented, harmonized standards are a way for a company to achieve compliance through self-assessment, provided that the exceptions mentioned are considered. This clearly seems to be the most cost-effective way for a company to achieve compliance, as there is then no mandatory requirement for notified bodies' consultations. Next,

two standards EN 18031-1:2024 and EN 18031-2:2024 which are relevant for this work are presented. EN 18031-3:2024 will be skipped, since its fraud protection requirements are explicitly stated to be considering internet connected radio equipment processing virtual money or monetary value. As a reminder, the limitations of Section 4 must be taken into account when assessing the standards. Annexes A.1, B.1 and C.1 are summaries created from these two standards. They introduce the most relevant requirements of these standards in more concise form.

EN 18031-1:2024

EN 18031-1:2024 standard sets baseline for cybersecurity measures for radio equipment that connects to the internet and aims to ensure network protection under RED Article 3(3) (d). Next, all requirements of the standard are summarized and the required information which the manufacturer must provide is also presented.

[ACM-1] Access control mechanism – Applicability of access control mechanism: The standard requires that the radio equipment must use access control mechanisms to manage entities' access to security and network assets. This requirement does not exist if (a) the asset is intended to be a public, (b) operational environment already limits access of asset to authorized entities or (c) access of asset is illegal to be controlled. [40]

All security and network assets in the equipment must be documented and via decision tree to indicate whether each asset requires access control mechanisms or whether it falls under the allowed exceptions described above. Each decision in decision tree must be justified. [40]

[ACM-2] Access control mechanism – Appropriate access control mechanism: ACM-1 sets conditions when access control mechanisms should be used but ACM-2 states which kind of control mechanisms should be used. ACM-2 requires that only authorized entities should have access to protectable security or network assets. [40]

This requirement focuses on the effectiveness of each access control mechanisms. The

standard defines implementation categories for common access control models, listed as an example role-based, discretionary, mandatory and other generic access control methods. The manufacturer must describe each access control mechanism, which is in use for each asset identified under ACM-1, explaining how it ensures only authorized access to assets based on the chosen model. Also, outcome of decision-tree analysis for each asset's access control must be documented with justifications of chosen path. [40]

[AUM-1-1, AUM-1-2] Authentication mechanism - Applicability of authentication mechanisms (network interfaces and user interfaces): Access control mechanisms required by ACM-1 must use authentication mechanisms for managing entities' access via network / user interfaces that allow them to (a) read confidential network function configuration or security parameters, (b) modify sensitive network function configuration or sensitive security parameters or (c) use network or security functions. The point (c) has two conditions when it is not applied. If access via those network / user interfaces (i) must be unauthenticated to enable the equipment's intended functionality or (ii) physical or logical measures in operational environment already limit the access to the authorized entities. [40]

All network / user interfaces should be identified and determined which of these provide access to previously described sensitive functions or data. Each interface must be documented whether the authentication is implemented or does it fall under the described exceptions. In technical documentation, each required access control which is utilizing network / user interface must be paired with a specific authentication mechanism and each relevant asset and access type is listed. [40]

[AUM-2] Authentication mechanism - Appropriate authentication mechanisms: Authentication mechanisms which are required by AUM-1-1 (network) and AUM-1-2 (user) must verify the entity's claim. This must be done by investigating evidence from at least one element of categories "knowledge", "possession" or "inherence". [40] The purpose of this requirement is to ensure that whenever authentication is used, it adheres to at

least basic best practice by using some recognized factor. For example, this is something the user knows, something the user has or something the user is.

A description of each used authentication mechanisms on the device must be provided, including which type of factor is used. Decision-tree evaluation must be also documented for each authentication mechanism to ensure that it meets set on-factor criteria. [40]

[AUM-3] Authentication mechanism - Authentication validation: Authentication mechanisms which are required by AUM-1-1 (network) and AUM-1-2 (user) must validate all relevant properties of the used authenticators which are aligned with the information available in the operational environment [40]. This requirement demands sufficient quality of authentication verification. Partial or too weak validation is not allowed.

A description for each authentication mechanism of how they validate the provided authenticator must be provided. This includes how the mechanism checks the credentials' properties and what those relevant properties are. [40]

[AUM-4] Authentication mechanism - Changing authenticators: There must be possibility to change the authenticator for authentication mechanisms required by AUM-1-1 (network) or AUM-1-2 (user) except if a conflicting security goal does not allow the change. [40] The device must support mechanisms which allows updating or replacing credentials so that static credentials are not permanent unless there is clear security goal which demands that they must stay fixed.

Descriptions of how user or administrator can change each authenticator must be provided. Also, if the authenticator can not be changed due to "conflicting" security goals, this must be also documented. [40]

[AUM-5-1] – Password strength (factory default passwords): If factory default passwords are used for authentication mechanisms of AUM-1-1 and AUM-1-2, they must be (a) unique per equipment and (b) follow best practice considering the strength of it or (c) it must be forced to be changed by the user. The manufacturer should employ one of these approaches and document which one is used. [40]

[AUM-5-2] – Password strength (non-factory default passwords): If non-factory default passwords are used for authentication mechanisms of AUM-1-1 and AUM-1-2, they must be (a) forced to be changed by the user or (b) defined by authorized entities within network where the access is limited to the authorized entities or (c) generated by the equipment with best practice strength and only communicating to an authorized entity within network of authorized entities. The manufacturer should employ at least one of these approaches and document which is used. [40]

[AUM-6] Authentication mechanism - Brute force protection: Authentication mechanisms which are required by AUM-1-1 and AUM-1-2 must be resilient against brute force attacks. The device must include prevention mechanisms that it is not possible to conduct unlimited amount of authentication attempts which could allow an attacker to guess credentials by trial and error. The manufacturer must provide document explaining what brute-force mitigation method is used. [40]

[SUM-1] Secure update mechanism - Applicability of update mechanism: There should be at least one update mechanism for updating software (including firmware) of the device affecting security assets and/or network assets with certain exceptions. The requirement does not apply if (a) functional safety considerations prohibit being updateable, (b) the equipment is immutable by its design or (c) the device is protected with other measures during its life cycle so that the updates are needless. [40]

The manufacturer is expected to inventory all software and firmware parts of the equipment that relate to security or networking. For each part, update method or exemption invoking must be documented. The documentation should include a list of all software components and indicate which are updateable and how, or why not. [40]

[SUM-2] Secure update mechanism - Secure updates: Update mechanisms of SUM-1 must only install software whose integrity and authenticity are valid at the time of installation [40]. This mandates that the update process must be secured. The updates must be verified so that unauthorized or tampered updates are not possible. Cryptographic

signatures or hash checks must be implemented for the updates. [40]

[SUM-3] Secure update mechanism - Automated updates: Update mechanisms of SUM-1 must fulfill certain requirements for updating the software. The update shall be performed (a) without human intervention at the equipment or (b) by scheduling the installation of update with human approval or (c) by triggering the installation of an update under human supervision to prevent unexpected damage in the environment. [40]

The device must support automated, or at least semi-automated, update process to ensure timely security updates. In practice, this means that once the update is available, the equipment can apply it either entirely automatically or with minimal user interaction. The manufacturer should document which kind of automated updates the product supports. The allowed three modes are (a) fully automatic, (b) scheduled or (c) user-approved trigger. [40]

[SSM-1] Secure Storage Mechanism – Applicability of secure storage mechanisms: Secure storage mechanisms must always be used to protect security assets and network assets that are stored persistently on the equipment, except when the operational environment's physical or logical measures protect that those assets are available only to authorized entities. [40] In practice, this requires that if the device keeps some kind of sensitive data in persistent memory of device, it must protect those assets e.g. via encryption or integrity controls unless it is guaranteed otherwise that the storage is not at risk.

The manufacturer must document all security assets and network assets stored in the persistent memory of device. For each, the documentation must indicate what secure storage mechanisms are used or why it is not needed due to the environment. [40]

[SSM-2] Secure Storage Mechanism – Appropriate integrity protection for secure storage mechanisms: Integrity of the security assets of SSM-1 must be protected by SSM-1 secure storage mechanisms. If secure storage mechanism is used, it must include measures that the data cannot be altered by an attacker without detection. The

documentation should include list of all assets under secure storage mechanisms and their integrity protection approach for each asset. [40]

[SSM-3] Secure Storage Mechanism – Appropriate confidentiality protection for secure storage mechanisms: The secure storage mechanisms of SSM-1 must protect secrecy of confidential security parameters and confidential network configuration that it stores persistently. [40] If certain data is identified as confidential, the storage mechanisms should keep it secret e.g. via encryption. Each secure storage mechanism which holds confidential data must be documented and explain how it ensures confidentiality. [40]

[SCM-1] Secure Communication Mechanism – Applicability of secure communication mechanisms: Secure communication mechanisms must always be used when the device communicates security assets or network assets with other entities via network interfaces. This requirement does not apply if (a) the communication of those assets is protected, with already discussed physical or logical measures that prevent unauthorized access in the environment. The requirement does not also apply if (b) the exposure of those assets is inherent to establishing or managing connections and it has also additional measures to establish trust. [40] In practice, whenever the device sends or receives security-sensitive or network-critical data over any network interface, the communication must be protected, unless the certain exceptions apply.

All interfaces carrying sensitive data must be listed and the type of data they carry on. For these, SCM must be employed and in the case where the exception applies, the documentation and decision described in the standard should justify it by one of the above exceptions. [40]

[SCM-2, SCM-3] Secure Communication Mechanism – Appropriate integrity, authenticity and confidentiality protection for secure communication mechanisms: Each SCM of SCM-1 must apply best practices to protect integrity, authenticity and confidentiality of communicated network assets and security assets where confidentiality is needed. This does not apply if divergence is needed for achieving interoperability. [40]

Details of used SCMs must be provided. The documentation and possibly a decision tree should indicate deviations from best practices with justifications. Used encryption mechanisms must be documented and if any part of communication is not encrypted, this must be justified. [40]

[SCM-4] Secure Communication Mechanism – Appropriate replay protection for secure communication mechanisms: Each SCM of SCM-1 must apply best practices to protect the network assets and security assets against replay attacks. This requirement does not apply if (a) a duplicate transmission does not pose a replay threat or (b) divergence is needed for achieving interoperability. The manufacturer must provide documents for each SCM how the replay is mitigated. [40]

[RLM-1] Resilience Mechanism – Applicability and appropriateness of resilience mechanisms: Resilience mechanisms which mitigate the effects of DoS attacks on its network interfaces must be used. The state of the device must return to defined state after an attack. This requirement does not apply for interfaces which (a) communicate only within local network or (b) where other devices in the network provide sufficient protection against DoS attacks. All network interfaces must be listed and describe resilience measures for each and also describe how the device recovers to the stable state. [40]

[NMM-1] Network Monitoring Mechanism – Applicability and appropriateness of network monitoring mechanisms: If the device is a network equipment, it must have network monitoring mechanisms to detect indicators of DoS attacks. For devices which this requirement does apply, types of traffic anomalies the equipment can detect must be documented. [40]

[TCM-1] Traffic Control Mechanism – Applicability of and appropriate traffic control mechanisms: If the device is a network equipment, it must have network traffic control mechanism. The manufacturer must describe the traffic control measures. [40]

[CCK-1] Confidential Cryptographic Keys – Appropriate Confidential Cryptographic Keys (CCKs): CCKs which are preinstalled or generated by the equipment dur-

ing its use must support minimum security strength of 112 bits, expect for CCKs that are used only by specific security mechanisms where aberrance is justified under ACM, AUM, SCM, SUM or SSM. [40]

All CCKs the equipment uses, and their strengths must be documented. If CCK does not meet the criteria of this requirement, it must be tied to the particular mechanism and explicitly justify the exception within that mechanism's context. [40]

[CCK-2] Confidential Cryptographic Keys – CCK generation mechanisms: The best practice cryptography must be followed in generation of CCKs expect for CCKs that are used only by specific security mechanisms where aberrance is justified under ACM, AUM, SCM, SUM or SSM. [40]

The manufacturer must describe the key generation process. If key generation differs from best practice, it must be in the respective mechanism's context. [40]

[CCK-3] Confidential Cryptographic Keys – Preventing static default values for preinstalled CCKs: Preinstalled CCKs must be practically unique for each equipment. This requirement does not apply if (a) if CCKs are only used for creating initial trust under conditions controlled by an authorized entry or (b) CCKs that are shared parameters which are essential for the equipment's intended functionality. [40]

The manufacturer must list all preinstalled CCKs and indicate which are unique per device. If CCK is not unique, it must be justified why it falls under the exceptions. [40]

[GEC] General Equipment Capabilities: The last chapter of standard consists of six general requirements. GEC-1 requires that the equipment must not contain publicly known vulnerabilities with certain exceptions where this requirement does not apply. GEC-2 states that in factory default state, the equipment must only expose network interface and services affecting security or network assets which are essential for setup or basic operation. GEC-3 requires that authorized use must have option to enable or disable optional interfaces or services exposed via network interfaces which are part of factory default state. GEC-4 requires that the user documentation must have a description of all

exposed network interfaces and services exposed via network interfaces which are part of the factory default state. GEC-5 demands that the equipment must not expose unnecessary physical external interfaces. GEC-6 sets requirement considering input validation. The equipment must validate input which it receives via external interface if the input could have potential impact on security assets or network assets. [40]

For GEC-1, manufacturer is expected to perform vulnerability monitoring on all software components, addressing them or accepting the risk under the exceptions. Acceptable risks must be risk managed. GEC-2 requires that the manufacturer must provide list of all network interfaces and network services which are enabled in the default configuration. For GEC-3, manufacturers must identify services and interfaces which are considered optional in the equipment's default state and confirm that the UI or other management interface provides controls for disabling those. Considering GEC-4, the user guide or manual of the equipment should contain section which enumerates interfaces. For GEC-5, the manufacturer must identify all physical external interfaces and justify each one's purpose. In this case, external means accessible from outside the product's casing, e.g. Ethernet jack, USB port or serial port. GEC-6 requires that manufacturer has designed the system with proper input validation and in the assessment, this is analyzed via code reviews or static analysis and eventually via dynamic testing. [40]

EN 18031-2:2024

Whereas EN 18031-1 takes stand for network, EN 18031-2 sets requirements considering personal data and privacy. EN 18031-2 includes also additional requirements for toys and human wearable devices. [ACM], [AUM], [SUM], [SSM], [SCM], [CCK], [GEC], [CRY] of EN 18031-1 are also presented in EN 18031-2 but since they are already set out, they are skipped here. Also, requirements considering children's toys and parental or guardian control for them are skipped due to their irrelevancy.

[LGM-1] Logging Mechanism - Applicability of logging mechanisms: For internal

activities which are concerning privacy assets and their protection, the equipment must use logging mechanisms. This does not apply if there is a legal obligation which denies logging activities. [41]

A description of each internal activity and the used logging mechanisms for the events which concern privacy assets and their protection must be provided. If the exception applies, the manufacturer must provide references to the legal documentation which shows how this is applicable for the equipment's internal activity. Descriptions of selected paths through the standard's decision tree for each event must be provided and justifications for the selected paths. [41]

[LGM-2] Logging Mechanism - Persistent storage of log data: Logging mechanisms of LGM-1 must store in the persistent storage of device all log data for related events. This does not apply if related log data is stored outside the equipment. [41]

The documentation must include a description of each logging mechanism of LGM-1 and detailing logged events and how the data is stored. If logs are stored in the equipment, the location and retention of this data should be explained. If logs are stored outside the equipment, the equipment's capability to support external log storage must be described. Descriptions of selected paths through standard's decision-making trees for each event must be provided and justifications for selected paths. [41]

[LGM-3] Logging Mechanism - Minimum number of persistently stored events: A minimum amount of the latest events and the latest event must always be included for log data stored in persistent storage by logging mechanisms of LGM-1. [41]

Events that are logged when data is persistently stored on the equipment must be described. Minimum amount of most recent events that can be stored simultaneously must be stated and the data's storage locations. Descriptions of selected paths through standard's decision-making trees for each event must be provided and justifications for selected paths. [41]

[LGM-4] Logging Mechanism - Time-related information of persistently stored

log data: A timestamp if real-time is available and time-related information if real time is not available must always be included for log data stored in persistent storage by logging mechanisms of LGM-1. [41]

Events that are logged when data is persistently stored on the equipment must be described. Each logging mechanism of LGM-1 must be described including details about real-time sources and their timestamps if the real-time data is available. If real-time data is not available, the stored time-related info must be described. Descriptions of selected paths through standard's decision tree for each event must be provided and also justifications for selected paths. [41]

[DLM-1] Deletion mechanism - Applicability of deletion mechanisms: There must be deletion mechanisms implemented in the equipment so that the user can delete their personal data and sensitive security parameters from the equipment [41].

The manufacturer must provide a description of the types of personal data and sensitive security parameters that can be stored in the equipment. Each deletion mechanism must be described and tell whether it deletes data by the user directly or indirectly via authorized entity behalf of the user. Descriptions of selected paths through standard's decision tree for each event must be provided and justifications for selected paths. [41]

[UNM-1] User notification mechanism - Applicability of user notification mechanisms: The equipment must inform user about changes which are affecting the protection or privacy of personal information. This does not apply if there are other methods informing users which do not require the equipment. [41]

A description of the types of personal data that can be stored in the equipment must be provided. For each use case that may impact privacy or data protection, manufacturer must describe how user is notified via the equipment. If the equipment is not involved with delivering the notification, the alternative method used must be described. Descriptions of selected paths through standard's decision tree for each event must be provided and justifications for selected paths. [41]

[UNM-2] User notification mechanism - Appropriate user notification content: The contents of notification of UNM-1 must include at least following data. A description about the change and a description of how the change affects the protection and privacy of personal information. [41]

Each user notification mechanisms of UNM-1 must be described. For each use case where notification is provided, the content of notification must be described. Descriptions of selected paths through standard's decision-making trees for each event must be provided and justifications for selected paths. [41]

5.2 Data Act

The Data Act is presented here as an indirect cybersecurity act because its main purpose is to regulate data sharing and products' users' rights for access and control of their data. Still, the Data Act can set requirements how this data should be shared, which both implicitly and explicitly addresses cybersecurity matters in terms of privacy. Figure 5.1 illustrates the Data Act.

5.2.1 Definitions

Next, the most relevant definitions of the Data Act are presented. These are essential to understand for the requirements mapping.

Data holder: "Data holder means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service" [42].

Product data: "Product data means data generated by the use of a connected product that the manufacturer designed to be retrievable, via an electronic communications

service, physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer" [42].

Readily available data: "Readily available data means product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation" [42].

Related service data: "Related service data means data representing the digitisation of user actions or of events related to the connected product, recorded intentionally by the user or generated as a by-product of the user's action during the provision of a related service by the provider" [42].

5.2.2 Requirements

Article 3 of the Data Act introduces pre-contract information duties for manufacturers. Article 3(2) requires that manufacturers of the connected products must tell users clearly such information:

- What data product can generate, its type, format and estimated volume
- Whether it generates data continuously and in real time
- Where the data is stored and its retention
- How the user can access, retrieve or delete the data

[43]

Article 3(3) requires that for the related services manufacturers must tell users clearly such information:

- Estimated volume, type and collection frequency of the product data and how the user can access it

- If data holder will use this data itself, the purpose must be described for the user and whether third parties are allowed to use the data.
- Identity of the data holder
- Contacts of the manufacturer
- How the user can request sharing with third parties

[43]

Data Act mandates that by default new products must be designed by default so that the product or service makes raw or pre-processed, readily available data, related service data and metadata easily, securely and free of charge available for the user. The data must be offered in structured, commonly used and machine-readable format and directly and in real-time where technically feasible. This applies from 12 September 2026. [43]

Even though access-by-design applies from 12 September 2026, user access right of the Data Act still applies already from 12 September 2025. If users can't directly access the data, manufacturers must still indirectly provide ways to access data. [44] Users must have access to data which their device co-generates from the use of connected device. Data holders must inform users about what data will be generated and how. Data holders must not use non-personal data without the user's consent. There is an exclusion that if confidentiality of the trade secrets is not preserved, there is no obligation for company to share inferred data. This only applies if company can demonstrate clearly that the trade secrets are endangered in data sharing. [31]

The Data Act sets requirements considering mandatory data sharing between businesses. When legally obligated, business must share data with other businesses on fair, reasonable and non-discriminatory (FRAND) terms. In this kind of situation, the company providing data may request reasonable compensation for providing data. Small and medium enterprises (SME) should not be overcharged from the data request. The Data Act sets also restrictions for data sharing between governments. There is a restriction that

non-personal data held in EU cannot be accessed by foreign government, unless there exists international agreement or certain legal conditions necessity, proportionality and transparency are met. [31] Also, this B2B request needs end-user's authorization or distinct agreement between companies for data sharing. The mandatory B2B sharing does not mean that companies can unilaterally and arbitrarily request data from other companies just because for developing competing products. [45]

The Data Act prohibits unilateral unfair terms in data sharing contracts, especially those affecting SMEs. The Data Act includes lists of these prohibited terms which are classified in two categories, "always considered to be unfair" and "presumed to be unfair". As a one listed example of "always considered to be unfair" is to exclude or even limit the liability of the party unilaterally imposing the condition for intentional conduct or gross negligence. [31]

The Data Act demands that data must be shared upon request of public authorities in case of an exceptional need. The exceptional need can be public emergencies, such as pandemics or natural disasters, and non-emergencies, such as statistical use. Still, the public sector must ensure that companies' trade secrets are protected, and the data is deleted after utilization. [31]

The Data Act sets obligations for data processing services. The Data Act mandates that data processing services must allow simple switching processes for their users if they want to switch service provider. This means that the data and the functionality must not be lost and from 12 January 2027, this should be allowed without charging any fees. During the transition period, providers should only charge cost-based fees from the switching process. [31]

The Data Act aims to enhance interoperability of data and set standards for data sharing. The Data Act introduces requirement that participants in data spaces must support interoperability and providers of smart contracts must enable automated execution of data-sharing agreements and withstanding of manipulation. [31]

There is one key carve-out which considers micro and small enterprises. Second chapter's obligations of the Data Act, which considers the data generated by the connected product, are excluded for the micro or small manufacturers or providers. [46]

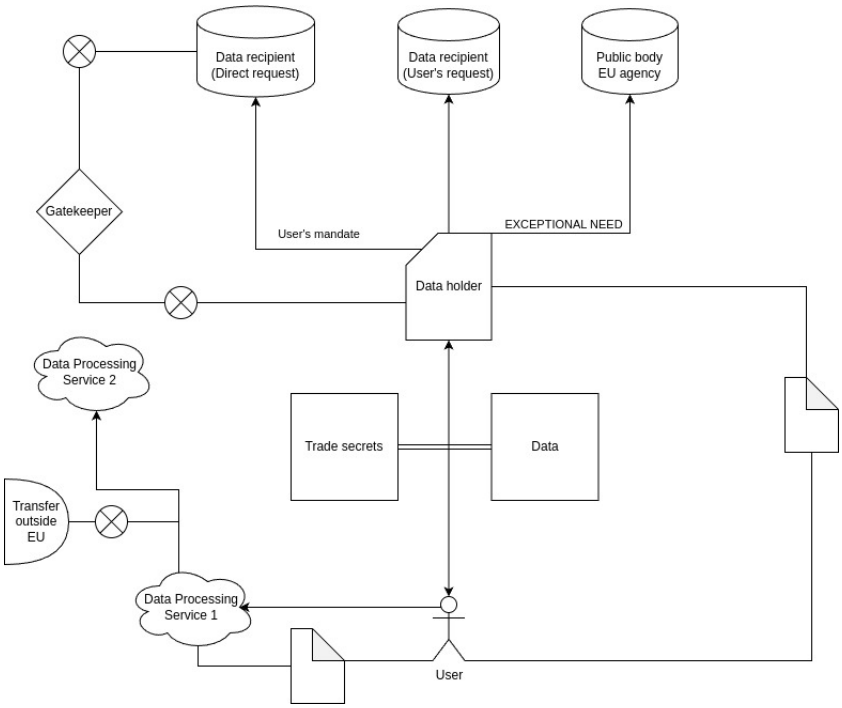

Figure 5.1: Data Act [47]

5.2.3 Compliance

Here, achieving compliance for the Data Act remains somewhat speculative since it does not have harmonized standards, nor common specifications for compliance. From the reviewed literature, it is seen that the burden of proof remains on the company, at least until the commission mandates the bodies to draft the standards. To summarize, it is suggested that the general principles and previously described requirements are followed.

5.3 CRA

Based on preliminary investigation in Section 4.4, CRA is considered a direct cybersecurity act since it sets explicitly actual cybersecurity requirements and because of the extent of the act, it is considered the most important upcoming act considering cybersecurity of software. The requirements of the act will now be considered. In this section, definition of the product defined in Section 4.4 applies.

5.3.1 Requirements

CRA sets obligations for manufacturers of the products. The obligations are grouped in essential cybersecurity requirements, cybersecurity risk assessment, technical documentation, declaration of conformity, information to users and notification requirements. [34] Next, key requirements of CRA are presented in groups.

A) Essential cybersecurity requirements for the products — Annex I, Part I

First, CRA obliges that products must have "appropriate level of cybersecurity" corresponding to the "risks". Appropriate level of cybersecurity is certainly ambiguous concept, and it is not elaborated in CRA in more detail. Another requirement is that product must be delivered "without any known exploitable vulnerabilities". Even though vulnerability is well-defined concept, definition of "known exploitable vulnerabilities" remains rather vague. [34]

Thirdly, CRA introduces specific cybersecurity measures which must be employed depending on risk assessment of Article 10(2) of CRA and where applicable. This is "where applicable" leaves, again, a lot of room for interpretation. It can not be concluded with full certainty whether this part means that if risk assessment does not require the requirement, it is not required to be fulfilled even though it is generally applicable or if the requirement is generally applicable no matter what the risk assessment states. How-

ever, CRA amplifies that there is pre-condition that these requirements are only applied when the product is installed, maintained, used to its intended purpose and under foreseen conditions. [34] The specific cybersecurity measures are discussed in more detail.

- **No known exploitable vulnerabilities (a):** The products must be delivered without any known vulnerabilities.
- **Secure by default (b):** The products must be delivered with secure configuration, and they must be possible to reset in their initial state.
- **Security updates (c):** Vulnerabilities must be possible to handle with security updates. Updates should be automatic by default.
- **Protection from unauthorized access (d):** Protection against unauthorized access must be ensured with authentication, identity or access management system and and possibility to report unauthorized access.
- **Protection of confidentiality of data (e):** Stored, transmitted or processed data should be encrypted or otherwise its confidentiality should be protected.
- **Protection of integrity of data (f):** Stored, transmitted or processed data and programs' integrity should be protected and reported.
- **Data minimization (g):** The product should only process the data which is strictly necessary for the product's intended purpose.
- **Availability of essential functions (h):** Availability of essential function during and after incidents must be ensured including resilience and mitigation against DoS attacks.
- **Minimizing negative impact (i):** Causing outages or problems for connected devices or networks must be avoided.

- **Limiting attack surfaces (j):** The products must be designed to reduce attack surfaces including external interfaces.
- **Exploit mitigation (k):** The products must be designed to reduce damage of incidents.
- **Security logging (l):** Internal activities like access or modifications should be recorded. An opt-out option for user must be provided.
- **Deleting data (m):** There should be possibility for user to securely and easily remove permanently all data and settings. [48]

B) Vulnerability handling process — Annex I, Part II

CRA requires that manufacturers must have processes for vulnerability handling for their products. Vulnerabilities must be identified, documented and patched with security updates. The manufacturers must test and review their products for vulnerabilities. They must provide enough information for users to fix found vulnerabilities and employ coordinated vulnerability disclosure policies (CVD policy). [34] Fixed vulnerabilities must be disclosed after the security update is available with details. Details should include impacts, severity and clear remediation info. The public disclosure may be delayed when it is justified in terms of security. [49]

CRA mandates that the vulnerabilities of the products must be patched for five years from the point where the product is placed on market or for the expected product lifetime. From these options, the shorter period is applied. When the lifetime is reasonably expected to be longer than five years, the manufacturers should provide longer support. [34]

CRA sets new obligations considering supply chain security. For instance, CRA mandates to maintain SBOM (Software Bill Of Material) for identifying vulnerabilities in third-party components. [50] SBOM is defined in the Article 3(39) as “a formal record

containing details and supply chain relationships of components included in the software elements of a product with digital elements" [43].

C) Manufacturer obligations considering organization and processes — Article 13

Manufacturers must perform and document cybersecurity risk assessments which include planning, designing, development, production, delivery and maintenance. The documentation must be kept updated during the support period on it should be included in the technical documentation. Any non-applicable essential requirements should be justified. Sufficient meticulousness must be exercised with third party components. Found vulnerabilities in the third-party components must be reported for their providers. [51]

Considering the previously discussed support period, the end date of support period must be published and, if possible, notify users on the product when supports ends. Security updates must be downloadable for at least 10 years after release or the remainder of the support period, whichever is longer. If significantly modified version of the software product is placed on the market, you are allowed support only the latest version if users of older version can upgrade their version to the latest version without extra costs. [51]

D) What must be given to users — Minimum contents of Annex II

Next is listed core information which should be supplied for the user of the product. User must be given manufacturer's name or trademark and contacts. Single Point of Contact (SPOC) for vulnerabilities and updates must be stated and link for manufacturers CVD policy must be offered. Users must be given product name and unique identification data. [52]

Users must be informed about the intended purpose of the product, its essential functions and security properties. Also assumed security environments must be described for the user. Foreseeable circumstances should be expressed which can lead to significant cybersecurity risks. [52]

Detailed instructions must be provided concerning secure commissioning and use of products, how changes affect the security, how security updates can be installed and how to turn off automatic security updates. Also, secure decommissioning and data removal must be described. SBOM could be made available for users and if so, information on how to access it must be told. [52]

E) What the technical documentation must contain — Annex VII

Technical documentation must contain general description including its purpose, relevant software versions, markings for hardware and user instructions. Design, development and production of the product and its vulnerability handling process must be described. Cybersecurity assessment must be included in the documentation and mapping of this assessment to the Annex 1 requirements. Rationale for support period must be included. Also, information concerning the conformity of the product should be included here. [53] Achieving conformity will be discussed later.

F) Mandatory reporting by manufacturers — Article 14

Manufacturers of the products must report certain information via ENISA's reporting to the designated Computer Security Incident Response Team (CSIRT) and ENISA [54]. Table 5.1 illustrates reporting requirements. The table is formed from CRA's Article 14's reporting requirements. On top of this chart, manufacturers of the products must inform users which are impacted, and when possible, all users with mitigation steps [54].

Information	**Actively exploited vulnerabilities**	**Severe incidents impacting the product's security**
Early warning	within 24 hours	within 24 hours
Notification	within 72 hours (general info, measures)	within 72 hours
Final report	14 days after patching or mitigating measure is available	within 1 month

Table 5.1: Manufacturers reporting requirements

5.3.2 Compliance

For Annex 1 in CRA which is listing the cybersecurity requirements, notified bodies can conduct conformity assessments but it can be done for the products internally by the manufacturer. There is presumption of conformity with Annex 1 requirements when products obey harmonized standards, common specifications or cybersecurity certification schemes. [34] Most of the products will fall into the group that manufacturers can self-declare compliance and the use of standards. There are no standards identified yet by European Standards Organizations (ESO). [55]

In Annex 3 of CRA, there are specified three classes of critical product types, two classes of important products with digital elements (Class 1 and Class 2) and one class of critical products. If the product falls into some of these classes, self-declaration is not sufficient. [55]

5.4 RPLD

For RPLD, there are no concrete requirements presented here, since there are not any. In Section 5.4 it is concluded that RPLD sets rules for the liability of manufacturers.

5.4.1 Compliance

As it is seen in Section 5.4, RPLD just sets rules considering manufacturers' liability. It does not necessarily mandate actual technical requirements, nor direct cybersecurity requirements. However, Doriana Cobârzan, Richard Bubel and Torsten Ullrich discuss in their article [39] how the RPLD still affects the software, and they introduce some key points which should be considered in terms of software.

An elimination of unnecessary software dependencies and non-essential libraries is suggested. Unnecessary dependencies increase attack surface and can potentially introduce security risks. [39]

The directive states that liability does not apply to free or open-source software outside of commercial activity. There is risk that in own software there can be risk of being liable for the damage unless the own product is not also distributed as non-commercial. [39] This is a risk which should be noted when open-source components are used as a part of own software.

As overall, even though there are no direct requirements for cybersecurity from the RPLD, Doriana Cobârzan, Richard Bubel and Torsten Ullrich see that in the future software quality will become increasingly important due to the directive, since it is punishable if the cybersecurity is not implemented at a sufficient level. They highlight the importance of dependency tracking and utilizing software quality assurance tools for identifying defects before the release of software.

6 Consequences for IoT and embedded devices

Based on the previously presented requirements of acts, summarizing consequences for IoT and embedded devices of acts' actions is now formed and we discuss RQ2. This generalization is made mainly based on IoT devices, since the literature is often referring to the IoT devices in general rather than embedded devices and because of motivation done in Section 2.1.2. Figure 6.1 summarizes complete timeline of relevant obligations for the manufacturers of the products.

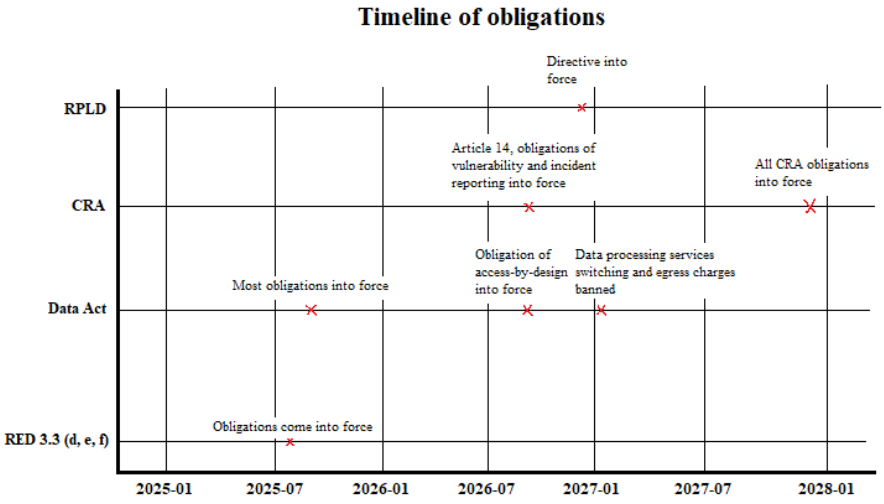

Figure 6.1: Timeline of obligations

6.1 RED Article 3(3)

As demonstrated in Section 5.1, complying with the new Article of RED is rather straightforward task, since there are already existing harmonized standards for self-assessment. Still, manufacturers must first define if their products fall under the scope of RED and which points of the article are concerning their products. Annexes A.1, B.1 and C.1 join the most relevant findings from the two harmonized standards. In addition, the exceptions defined in Section 4.2 must be considered when identifying whether self-assessment can be done or is the help of notified body needed.

6.2 Data Act

The Data Act mentions requirements specifically for IoT devices and it must be noted by the manufacturers of IoT products. As demonstrated in previous sections, there are found no technical requirements considering software implementation in terms of cybersecurity. Summarizing the findings in previous sections, the Data Act sets requirements for what data should be shared, when it must be shared and how. These requirements have implications for concrete software implementation. However, there are no implications that the Data Act would specify how the data should be secured and possible implementations for this. The Data Act editorializes only that trade secrets and personal data must be protected and again the only thing is that the Data Act sees these situations as places where data must not be shared for other actors.

The key factor for the Data Act's obligations is the definitions of it. For instance, many obligations considering data sharing are issued for the "data holders" and specifically concern "product data". This is important for the manufacturers to conclude whether they or their products fall under these definitions.

Another key take away for the Data Act is also the exclusions of SMEs, or even for micro enterprises. As presented in in Section 5.2.2, there are obligations which are not

considering SMEs or the obligations are at least loosened compared to large enterprises. Based on this, the Data Act apparently tries to reinforce the position of SMEs compared to large enterprises in the data economy. For manufacturers of the software product, this is important point to consider whether their company falls under the definition SME, or even under the definition of micro enterprise.

Even though the Data Act does not introduce cybersecurity requirements for the software, it has one potential cybersecurity related topic which should be paid attention to. As demonstrated in 5.2.2, the Data Act defines lot of new data sharing obligations. For instance, the Data Act establishes data sharing obligations between businesses and governments. This brings out concerns about the privacy.

6.3 CRA

Investigation done in Section 5.3 demonstrates that CRA introduces the most obligations for products with digital elements and therefore it considers also heavily cybersecurity of IoT and embedded devices. The done investigation shows that there are some similar overlapping properties with RED's requirements even though RED issues obligations for radio equipment. Table 6.1 summarizes the key obligations of CRA which are discussed in more detail in Section 5.3.

Obligation	**Key take away of the obligation**
A) Essential cybersecurity requirements for the products	Certain cybersecurity measures must be applied to the products based on risk assessment.
B) Vulnerability handling process	Manufacturers must have vulnerability handling process, where vulnerabilities are identified, documented and patched with security updates.
C) Manufacturer obligations concerning organization and processes	Manufacturers must perform risk assessment throughout the whole life cycle of the product and keep their documentation updated. The support period of the product must be clearly informed.
D) What must be given to users	User must be informed about the intended use of the product and its security environment. Details of safe use and commissioning must be described.
E) What the technical documentation must contain	Design, development and production of the product and its vulnerability handling process must be described.
F) Mandatory reporting by manufacturers	Certain information must be reported for ENISA and CSIRT.

Table 6.1: Summary of the obligations based on 5.3

CIA triad plays crucial role in CRA and the essential requirements of CRA are there for fulfilling the properties of CIA triad. CRA defines requirements to achieve properties of CIA triad and sufficient cyber resilience, but its requirements stay at a general level in CRA. It does not provide actual concrete solutions for achieving them. For instance, in the USA there is "US IoT Act" which obligates NIST to release and update standards considering IoT devices cybersecurity. These standards should be updated every five years, and they are considered as best practices to manufacture and secure IoT devices. [34] As previously touched in Section 5.3.2, there are no standards identified yet for CRA. This can be one reason for its current insufficiency. For larger companies these requirements might be a smaller burden compared to SMEs. They have already experience of designing their products while following secure by design principle which will be major challenge for SMEs. [55]

6.4 RPLD

The importance of RPLD should be highlighted in terms of the cybersecurity of the software. As stated in Section 5.4, RPLD does not bring out direct cybersecurity requirements, but it has certainly important derivative effect for IoT and embedded devices. Since it sets out explicitly terms considering the liability of manufacturers of products, and more precisely now even for the software products, manufacturers must implement their products' cybersecurity at sufficient level.

6.5 Additional takeaways

To summarize this whole regulatory burden, there is a lot of vagueness. For instance, considering the literature review of this thesis, there was no material found for compliance of the RED's Article's 3.3 new points. This is probably because RED recommends obeying harmonized standards if it is possible for manufacturers. Obeying these can be seen

as straight-forward task and there is no need for interpretation. As seen in Section 5.1, standards include very detailed descriptions of how some parts of software must be implemented for declaring sufficient conformity. However, the vagueness starts when there are no standards present. As seen in Section 5, lot of requirements are stated or presented but there is no hands-on guidance how these requirements are fulfilled. Also, the done investigation found no indication that data ownership matters would matter in terms of the obligations. How does the Data Act cope with situations where the user of connected product already owns the data and the manufacturer has just access to the data of device?

Also, it is worth noticing that this work did not find any new cybersecurity acts issued by EU which are specifically considering embedded or IoT devices. The same acts apply to IoT devices as to all other software products. The Data Act is the only such act, but it does not address direct cybersecurity matters.

7 Conclusion

This thesis mapped out the effects of EU's new upcoming cybersecurity related acts on the software solution of the IoT products. The thesis delved into the concrete requirements of the acts in detail and aims to highlight points for product manufacturers that they need to consider in order to achieve compliance considering their products' software solutions. The conducted investigation created a more readable summary of the future acts' impact which manufacturers can utilize when assessing the impact first time on their products without the laborious interpretation of legal text. The key take away from this thesis is the compiling of the concrete consequences for device manufacturers, which they can use when assessing the workload and practical consequences of the acts. Next, we discuss the research questions of this thesis and then we present the conclusions.

7.1 RQ 1

Which acts have an effect on IoT and embedded devices' software's cybersecurity?

The initial starting point for thesis was to start with preliminary investigation to gather information about presumable cybersecurity acts which could presumably affect the IoT and embedded devices' cybersecurity. Considering one investigated act, it is found relatively little relevance to cybersecurity.

Based on the investigation done, the Data Act has little direct effect or mandated requirements in terms of cybersecurity. In preliminary investigation, there was strong assumption that Data Act would regulate also protection of the data on top of its sharing

obligation. In the thesis, there are found no concrete requirements for how the data and its sharing should be protected in the Data Act. In Section 4.3 it is pointed out that GDPR rules personal data protection. Also as presented in Section 5.2.2, the Data Act states that data should be shared "securely". However, it does not specify in more detail what securely actually means.

In the thesis there are three identified acts which do have an actual effect on IoT and embedded devices' cybersecurity. These acts are RED, CRA and RPLD. RED and CRA are seen direct cybersecurity acts which directly issue cybersecurity requirements in terms of software solutions. RED expressly concerns radio equipment, and it is not concerning all IoT and embedded devices. Based on the extent of CRA, it will be the most relevant cybersecurity act of all reviewed acts.

The definition of product in RPLD is presented in Section 5.4 and because its broad definition, RPLD basically concerns all manufactured products in the EU. Investigation in this thesis demonstrated that it has indirect effect on products' cybersecurity, since extended liability will generally put even more pressure on the manufacturers to keep their products' security at sufficient level.

7.2 RQ 2

What are the consequences of the new upcoming acts for the devices' software and the manufacturers of these devices?

The individual acts' concrete consequences are presented in Section 6 but now we summarize them as overall. Based on the done investigation, it is seen that acts can cause documentation burden for companies. For instance, the contents of the standards of RED which are considered in this thesis demonstrate clearly that even though in the situation where manufacturers have already considered their products' cybersecurity and implemented it at sufficient level in terms of new acts, there is a burden of documentation

and preparation for declaring conformity which comes with the new acts. This similar documentation burden is expected to become with CRA also because, as stated before, it is declared that there is request for standardization bodies to implement standards.

7.3 Restrictions

The major restriction in this work is that the ground and the acts are based on the real-world company's one specific IoT product which is the ventilation unit. The ventilation unit represents a technological solution which can be seen quite usual in nowadays technology industry's product. However, this base sets some restrictions and limits scope for done investigation which should be noted. As noted before, some cybersecurity related acts are excluded due to the preliminary investigation of Company X, listed as an example NIS2.

One restriction of this thesis is that it does not editorialize specific groups of IoT or embedded devices which might fall under additional acts. It is certain that the devices which are integrated into critical infrastructure or are medical devices, must have stricter requirements and own acts which should be conformed. These are excluded from this work. Another key restriction for this thesis is that it concentrates only software solutions of IoT products and just touches hardware side of the products.

Since this work was about summarizing the key findings from the acts, there is possibility that some obligations are missing from the done investigation. Also, it must be clarified that author of this thesis is not a lawyer. The thesis includes lot of interpreting of legislation texts of the EU and the conducted analysis in this thesis aims to remain rather too narrow than making too long invalid conclusions.

References

[1] I. Kamara, "European cybersecurity standardisation: A tale of two solitudes in view of europe's cyber resilience", *Innovation: The European Journal of Social Science Research*, vol. 37, no. 5, pp. 1441–1460, 2024. DOI: 10.1080/13511610.2024.2349626.

[2] European Parliament and Council of the European Union, *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, L 333, pp. 1-79. Text with EEA relevance, Dec. 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.

[3] European Commission. "NIS2 Directive: new rules on cybersecurity of network and information systems". (2023), [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (visited on 03/30/2025).

[4] L. Futcher and R. von Solms, "Guidelines for secure software development", in *Proceedings of SAICSIT 2008*, Wilderness Beach Hotel, Wilderness, South Africa: ACM, Oct. 2008, pp. 56–65, ISBN: 978-1-60558-286-3. DOI: 10.1145/1456659.1456667.

[5] V. Boppana, "Secure practices in software development", *Global Research Review in Business and Economics (GRRBE)*, vol. 10, no. 5, pp. 216–228, 2024, ISSN: 2454-3217 (Online), 2395-4671 (Print). DOI: https://doi.org/10.56805/grrbe.24.10.5.75.

[6] *Iot embedded systems*, CSJM University, Kanpur, 2023. [Online]. Available: https://gyansanchay.csjmu.ac.in/wp-content/uploads/2023/06/IoT-Embedded-Systems.pdf (visited on 03/30/2025).

[7] S. R. Yadav, N. D. Kalokar, R. D. Ade, A. P. Kasambe, V. S. Patale, and A. P. Yewale, "An embedded system", *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 4, no. 2, pp. 87–93, Feb. 2024. DOI: 10.48175/568. (visited on 03/30/2025).

[8] N. A. Yekini, O. A. Oloyede, A. Akinwole, and A. O. Akinade, "Overview of embedded system & its application", in *3rd International Academic Conference: Technical Education and Innovation – Trajectory for Sustainable National Development in the Face of Contemporary Global Challenges*, Academic Staff Union of Polytechnics, Iree Chapter, May 2022. [Online]. Available: https://www.researchgate.net/publication/361562662_OVERVIEW_OF_EMBEDDED_SYSTEM_ITS_APPLICATION (visited on 03/30/2025).

[9] J. Valvano and R. Yerraballi, "Introduction to embedded systems", in Austin, TX 78712, The United States: The University of Texas at Austin, 2022, ch. 2, pp. 69–107.

[10] IBM. "What is the internet of things (iot)?", IBM. (May 2023), [Online]. Available: https://www.ibm.com/think/topics/internet-of-things (visited on 03/30/2025).

[11] J. Valvano. "Embedded system block diagram". (2023), [Online]. Available: https://users.ece.utexas.edu/~valvano/mspm0/ebook/Ch1_files/EmbeddedSystemBlock.png (visited on 04/01/2025).

[12] A. Ramirez, A. Aiello, and S. J. Lincke, "A survey and comparison of secure software development standards", in *13th CMI Conference on Cybersecurity and Privacy (CMI)*, IEEE, 2020, ISBN: 978-1-7281-9056-3. DOI: 10.1109/CMI51275.2020.9322704.

[13] A. Hudaib, M. A. Alshraideh, O. Surakhi, and M. Alkhanafseh, "A survey on design methods for secure software development", *International Journal of Computers and Technology*, vol. 16, no. 7, pp. 7047–7063, Dec. 2017. DOI: 10.24297/ijct.v16i7.6467.

[14] "Cia-oposite". (Aug. 2017), [Online]. Available: https://thorteaches.com/wp-content/uploads/2017/08/CIA-OPOSITE.png (visited on 04/11/2025).

[15] H. Nina, J. A. Pow-Sang, and M. Villavicencio, "Systematic mapping of the literature on secure software development", *IEEE Access*, vol. 9, pp. 36 852–36 867, 2021. DOI: 10.1109/ACCESS.2021.3062388.

[16] J. Grégoire, K. Buyens, B. D. Win, R. Scandariato, and W. Joosen, "On the secure software development process: Clasp and sdl compared", in *29th International Conference on Software Engineering Workshops (ICSEW'07)*, Leuven, Belgium: IEEE, 2007, ISBN: 0-7695-2830-9. DOI: 10.1109/SESS.2007.7.

[17] A. Dessiatnikoff, "Vulnerabilities analysis of embedded avionic systems : Classification and experiment", Jul. 2014.

[18] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem", *Medical Devices: Evidence and Research*, vol. 8, pp. 305–316, 2015. DOI: 10.2147/MDER.S50048.

[19] D. Papp, Z. Ma, and L. Buttyán, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy", in *2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST)*, IEEE, 2015, pp. 145–152, ISBN: 978-1-4673-7828-4. DOI: 10.1109/PST.2015.7232966.

[20] H. Carrapico and B. Farrand, "Cybersecurity trends in the european union: Regulatory mercantilism and the digitalisation of geopolitics", *JCMS: Journal of Common Market Studies*, vol. 62, no. S1, pp. 147–158, 2024. DOI: 10.1111/jcms.13654.

[21] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review", *Sensors*, vol. 23, no. 8, p. 4117, 2023. DOI: 10.3390/s23084117.

[22] European Union. "Legal acts – glossary of summaries", EUR-Lex. (2025), [Online]. Available: https://eur-lex.europa.eu/summary/glossary/legal_acts.html (visited on 07/01/2025).

[23] European Union. "Directive (eu) – glossary of summaries", EUR-Lex. (2024), [Online]. Available: https://eur-lex.europa.eu/summary/glossary/directive.html (visited on 07/01/2025).

[24] European Union. "Regulation (eu) – glossary of summaries", EUR-Lex. (2025), [Online]. Available: https://eur-lex.europa.eu/summary/glossary/regulation.html (visited on 07/01/2025).

[25] European Union. "Standardisation – eur-lex glossary of summaries", EUR-Lex. (2025), [Online]. Available: https://eur-lex.europa.eu/EN/legal-content/glossary/standardisation.html (visited on 07/01/2025).

[26] European Parliament and Council of the European Union, *Directive 2014/53/eu of the european parliament and of the council of 16 april 2014 on the harmonisation of the laws of the member states relating to the making available on the market of*

radio equipment and repealing directive 1999/5/ec, Official Journal of the European Union, L 153, 22 May 2014, pp. 62-106., 2014. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053.

[27] Liikenne- ja viestintävirasto Traficom. "Radiolaitteiden tietoturvavaatimukset täsmentyvät – tarkista tuotteen vaatimustenmukaisuus ajoissa". (Feb. 10, 2025), [Online]. Available: https://www.traficom.fi/fi/ajankohtaista/radiolaitteiden-tietoturvavaatimukset-tasmentyvat-tarkista-tuotteen (visited on 02/17/2025).

[28] European Commission, *Commission delegated regulation (eu) 2023/2444 of 20 july 2023 amending delegated regulation (eu) 2022/30 as regards the date of application of the essential requirements for radio equipment and correcting that regulation*, 2023. [Online]. Available: http://data.europa.eu/eli/reg_del/2023/2444/oj.

[29] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, "Guidance on the application of the harmonised standards series en 18031:2024 in support of commission delegated regulation 2022/30", European Commission, Brussels, Belgium, Tech. Rep., 2024.

[30] M. Hennemann, G. K. Ebner, B. Karsten, G. Lienemann, and M. Wienroeder, *Data Act: An Introduction*. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2024, ISBN: 978-3-7560-1342-5. DOI: 10.5771/9783748918691.

[31] European Commission. "Data act explained", European Union. (2025), [Online]. Available: https://digital-strategy.ec.europa.eu/en/node/12633/printable/pdf (visited on 05/08/2025).

[32] D. Redli, "Rights of users to data generated by iot devices", LL.M. Thesis, Faculty of Law, Masaryk University, Brno, Czech Republic, 2023, p. 97.

[33] "Eu data act, Updates, compliance". (), [Online]. Available: https://www.eu-data-act.com (visited on 06/01/2025).

[34] M. R. Shaffique, "Cyber resilience act 2022: A silver bullet for cybersecurity of iot devices or a shot in the dark?", *Computer Law & Security Review*, vol. 54, p. 106 009, 2024. DOI: 10.1016/j.clsr.2024.106009.

[35] European Parliament and Council of the European Union, *Article 3: Definitions*, Article 13, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[36] Liikenne- ja viestintävirasto Traficom. "Cyber resilience act, cra". (2025), [Online]. Available: https://kyberturvallisuuskeskus.fi/en/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra (visited on 08/09/2025).

[37] Liikenne- ja viestintävirasto Traficom. "Timeline of the cyber resilience act (cra)". (2025), [Online]. Available: https://kyberturvallisuuskeskus.fi/sites/default/files/styles/media_image_lg/public/media/images/cra_aikajana_eng_web.jpg (visited on 08/09/2025).

[38] C. Kiefer and L. Herlitz. "Liability for software under the new european product liability directive". (Apr. 30, 2025), [Online]. Available: https://www.ibanet.org/European-Product-Liability-Directive-liability-for-software (visited on 06/27/2025).

[39] D. Cobârzan, R. Bubel, and T. Ullrich, "The impact of the european product liability directive on software engineering", in *Proceedings of the 20th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE*

2025), Lisbon, Portugal: SCITEPRESS, 2025, pp. 626–634, ISBN: 978-989-758-742-9. DOI: 10.5220/0013363100003928.

[40] *Common security requirements for radio equipment, Part 1: Internet-connected radio equipment*, European Standard, Aug. 14, 2024. [Online]. Available: https://standards.iteh.ai/catalog/standards/cen/4f1e2768-e1a6-4541-a2b6-465e1c682627/en-18031-1-2024.

[41] *Common security requirements for radio equipment, Part 2: Radio equipment processing data, namely internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment*, European Standard, Aug. 14, 2024. [Online]. Available: https://standards.iteh.ai/catalog/standards/cen/bc3fd947-d9dc-42ac-9156-ed13b9e14965/en-18031-2-2024.

[42] European Parliament and Council of the European Union, *Regulation (eu) 2023/2854 (data act) — article 2: Definitions*, EU regulation, Dec. 22, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (visited on 08/22/2025).

[43] European Parliament and Council of the European Union, *Regulation (eu) 2023/2854 (data act) — article 3: Obligation to make product data and related service data accessible to the user*, EU regulation, Dec. 22, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (visited on 08/22/2025).

[44] European Parliament and Council of the European Union, *Regulation (eu) 2023/2854 (data act) — article 4: The rights and obligations of users and data holders with regard to access, use and making available product data and related service data*, EU regulation, Dec. 22, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (visited on 08/22/2025).

[45] European Parliament and Council of the European Union, *Regulation (eu) 2023/2854 (data act) — article 6: Obligations of third parties receiving data at the request of the user*, EU regulation, Dec. 22, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (visited on 08/22/2025).

[46] European Parliament and Council of the European Union, *Regulation (eu) 2023/2854 (data act) — article 7: Scope of business-to-consumer and business-to-business data sharing obligations*, EU regulation, Dec. 22, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (visited on 08/22/2025).

[47] C. Gallese. "The framework of the data act". (2022), [Online]. Available: https://www.researchgate.net/figure/The-framework-of-the-Data-Act_fig1_365680045 (visited on 05/25/2025).

[48] European Parliament and Council of the European Union, *Annex i – part i: Cybersecurity requirements relating to the properties of products with digital elements*, Annex I – Part I, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[49] European Parliament and Council of the European Union, *Annex i – part ii: Vulnerability handling requirements*, Annex I – Part II, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[50] J. Ruohonen and P. Timmers. "Vulnerability coordination under the cyber resilience act". (2024), [Online]. Available: https://arxiv.org/abs/2412.06261 (visited on 07/01/2025).

[51] European Parliament and Council of the European Union, *Article 13: Obligations of manufacturers*, Article 13, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[52] European Parliament and Council of the European Union, *Annex ii: Information and instructions to the user*, Annex II, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[53] European Parliament and Council of the European Union, *Annex vii: Content of the technical documentation*, Annex VII, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[54] European Parliament and Council of the European Union, *Article 14: Reporting obligations of manufacturers*, Article 14, Regulation (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements, Oct. 23, 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[55] P. Schoo, "Navigating the cra: A brief analysis of european cyber resilience act and resulting actions for product development", in *Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS 2024)*, Setúbal, Portugal: SCITEPRESS – Science and Technology Publications, Lda., 2024, pp. 245–251, ISBN: 978-989-758-699-6. DOI: 10.5220/0012690500003705.

Appendix A Summary of EN 18031-1:2024 (1/2)

Requirement	Core obligation	Required manufacturer documentation
ACM-1	Use access control for security/network assets unless public, environment-limited, or unlawful to control	Asset inventory; decision-tree per asset with justification; record exceptions
ACM-2	Ensure only authorized entities can access protectable assets; suitable model	Mechanism per asset; chosen model; rationale; decision-tree outcome
AUM-1-1 / AUM-1-2	Enforce authentication on network/user interfaces that read/modify sensitive items or use security/network functions (with limited exceptions)	List all interfaces; mark where authentication applies vs. exception; map each required access control to a specific authentication mechanism
AUM-2	Verify identity using 1 factor (knowledge/possession/inherence)	Describe authentication mechanism and factor types; show compliance decision-tree
AUM-3	Validate relevant properties of authenticators	How each mechanism validates credentials and which properties
AUM-4	Authenticators must be changeable unless there is conflicting security goal	How to change each authenticator; justify any non-changeable cases
AUM-5-1	Factory default passwords: unique per device, or strong, or forced change	Chosen approach and rationale
AUM-5-2	Non-factory passwords: forced change; or set in controlled network; or device-generated strong	Chosen approach and controls
AUM-6	Brute-force resilience	Explain mitigation method(s)
SUM-1	Provide at least one update mechanism for security/network-relevant software (with some exceptions)	SBOM of relevant software; per item: update method or justified exemption
SUM-2	Install only updates with verified integrity/authenticity	Verification flow; crypto controls; failure handling
SUM-3	Support automatic, scheduled-with-approval, or user-triggered-supervised updates	State supported mode(s) and controls

Table A.1: EN 18031-1:2024 — Obligations and documentation (1/2)

Appendix B Summary of EN 18031-1:2024 (2/2)

Requirement	Core obligation	Required manufacturer documentation
SSM-1	Protect at-rest security/network assets in persistent storage (unless environment guarantees authenticated access)	List stored assets; chosen storage protections or justified exception
SSM-2	Integrity protection for SSM-1 assets	Per asset: integrity controls (signatures, etc.)
SSM-3	Confidentiality for confidential parameters/configs	Per mechanism: encryption/key management details
SCM-1	Protect communication of security/network assets over network interfaces (with limited exceptions)	List sensitive-data interfaces; apply SCM or justify exception path
SCM-2 / SCM-3	Best-practice integrity, authenticity, confidentiality; limited interoperability deviations	Protocols/key lengths; document deviations and reasons
SCM-4	Replay protection where threat exists; exceptions if no replay risk or interoperability need	Replay mitigation per interface
RLM-1	DoS resilience on network interfaces; recover to defined state	Per interface: resilience measures and recovery behavior
NMM-1	Detect indicators of DoS (network equipment)	Detection capabilities; anomaly types
TCM-1	Traffic control mechanisms (network equipment)	Describe traffic control measures
CCK-1	CCKs 112-bit strength; exceptions only when tied/justified in related mechanisms	List all CCKs with strength; map/justify any exception
CCK-2	Best-practice CCK generation	Describe generation process; note contextual deviations if any
CCK-3	Preinstalled CCKs practically unique per device (narrow exceptions)	List preinstalled CCKs; mark uniqueness; justify shared keys
GEC-1	No publicly known vulnerabilities (managed/justified exceptions)	Vulnerability monitoring/handling; risk acceptance records
GEC-2	Default exposes only essentials for setup/basic operation	List default-enabled interfaces/services
GEC-3	Users can enable/disable optional default services/interfaces	Evidence of UI/management controls
GEC-4	Documents list default-exposed interfaces/services	Manual/user guide excerpts
GEC-5	No unnecessary physical external interfaces	List physical interfaces with purpose/justification
GEC-6	Validate external inputs impacting security/network assets	Design description; code review/static/dynamic test evidence

Table B.1: EN 18031-1:2024 — Obligations and documentation (2/2)

Appendix C Summary of EN 18031-2:2024

Requirement	Core obligation	Required manufacturer documentation
LGM-1	Log internal activities related to privacy assets and their protection (unless legally prohibited)	Describe activities and logging; cite legal basis if exception; decision-tree path/justification
LGM-2	Persist related log data on device	Where/how stored (on-device vs. external), retention; decision-tree path
LGM-3	Retain a minimum set of most recent events and always the latest event	Minimum capacity and storage location; decision-tree path
LGM-4	Include timestamp (if real-time available) or time-related info otherwise	Real-time source or alternative time metadata; decision-tree path
DLM-1	Provide mechanisms for users to delete personal data and sensitive security parameters	Catalogue of data/SSP types; deletion workflows (direct/via authorized entity); decision-tree path
UNM-1	Notify users of changes affecting protection/privacy of personal data (or use an alternative method)	Notification channels per use case or alternative method; decision-tree path
UNM-2	Notification content must include description of change and its impact on protection/privacy	For each use case: content elements included; decision-tree path

Table C.1: EN 18031-2:2024 — Obligations and documentation