Developing with Compliance in Mind: Addressing Data Protection Law, Cybersecurity Regulation, and AI Regulation During Software Development

Bjørn Aslak Juliussen[1][0000−0003−0046−8263] ⋆, Jon Petter Rui[2,3][0000−0001−7629−1834], and Dag Johansen[1][0000−0001−7067−6477]

[1] Department of Computer Science, UiT The Arctic University of Norway, Tromsø, Norway
[2] Faculty of Law, University of Bergen, Norway
[3] Faculty of Law, UiT The Arctic University of Norway, Tromsø, Norway

Abstract. **Keywords:** Personal Data Protection · Cybersecurity Regulation · Artificial Intelligence Regulation · Security Measures for the Protection of Personal Data

1 Introduction

In the past decade, the software industry has experienced an increase in technology-related regulations from the European Union (EU), highlighting the importance of incorporating legal requirements into the software system development process. It is complex and challenging to retrospectively retrofit security and data protection constraints into existing deployed software systems. Hence, this paper focuses on the concept of implementing compliance requirements as early as possible in the software system development process.

Non-functional requirements, which refer to the overall properties of a software system rather than specific features of the system [1], are critical to consider and implement during software system development. Privacy and security are two examples of non-functional properties. Privacy and data protection are primarily addressed in the General Data Protection Regulation (GDPR) [2]. The GDPR has made an important impact on the development processes of software systems across the EU member states since it entered into force in 2018 [11,12,13]. A somewhat similar regulatory impact with regard to cybersecurity has entered into force in the EU in January 2023 [3] and will potentially have a comparable effect on software development and deployed software systems in the sectors where the directive comes into effect.

By the 18$^{\text{th}}$ of October 2024, the EU member states must adopt the requirements in the Network and Information Security (NIS) 2 Directive [3]. The NIS 2 Directive requires that operators of essential services for society – e.g. health care providers, energy sector entities, and food distributors – must conduct risk

⋆ Corresponding author. Email: bjorn.a.juliussen@uit.no

analyses of their networks and information systems, and have measures for incident handling and crisis management. If an essential entity is non-compliant with the NIS 2 Directive, they risk fines of up to 10 million euros or 2 % of total worldwide annual turnover, under the NIS 2 Directive Article 31(4).

A proposal for a specific Artificial Intelligence regulation, known as the AIA [4], is also emerging in the EU, and the AIA will most likely enter into force within a couple of years after the end of the trialogue negotiations and the legislative process [5]. Providers placing a non-compliant AI system on the market in the EU risk fines of up to 30 million euros or 6 % of total worldwide annual turnover, under the proposed AIA Article 71(3).

The paper addresses one important initial part of developing compliant software systems, namely, how to ensure concurrent compliance with multiple regulations when a software system enters the scope of several regulations. In order to assess this question, it is necessary to analyse whether the GDPR and the NIS 2 Directive have conflicting requirements and whether there are differences in the cybersecurity concept across the NIS 2 Directive and the proposed AIA. The relevance of the questions examined could be illustrated through the following example:

Consider an entity operating in a critical sector, such as healthcare or energy, within an EU member state, which processes personal data. As a result, the entity falls under the scope of both the GDPR and the NIS 2 Directive. To address cybersecurity concerns, the entity decides to implement an adaptive authentication system [20] that calculates the risk of the user being an adversary attacker. The system estimates risk based on various types of personal data that the system processes, such as time of day, location, device status, and end-user behaviour. The risk score is calculated based on a machine learning (ML) model. In this scenario, the GDPR applies due to the processing of personal data, the NIS 2 Directive applies due to the entity being a critical sector entity, and the proposed AIA applies due to the risk being calculated with a ML model. The paper will examine the overlapping scope of these regulations and analyse how to potentially achieve concurrent compliance.

The paper is structured as follows: Section 2 analyses the overlapping scope of the GDPR and the NIS 2 Directive and focuses on the research question of whether there are any potential conflicting requirements between the two rule sets. Section 3 examines the overlapping scope of the AIA and the NIS 2 Directive and analyses whether there are differences in the cybersecurity concept across the NIS 2 Directive and the proposed AIA. Section 4 discusses the overall findings and concludes with a set of suggestions for software systems developers for concurrent NIS 2, GDPR, and AIA compliance.

2 The Scope of the NIS 2 Directive and the GDPR

2.1 The Material Scope of the NIS 2 Directive

Traditionally, the concepts of cybersecurity and data protection possess distinct objectives and attributes, and in certain scenarios, they may appear to be in

opposition to each other [21]. For instance, consider a scenario where personal data is securely stored and encrypted within an organisation. In this case, the data is protected with an appropriate level of security. However, the processing could still violate the provisions of the GDPR if, for example, the processing of personal data lacks a valid legal basis under Article 6(1) GDPR or if the data is stored in breach of the principle of storage limitation. This section will analyse the joint scope of the NIS 2 Directive and the GDPR and assess the potential for conflict between the two legal frameworks.

The primary objective of the NIS 2 Directive is to enhance the overall level of cybersecurity in the EU member states through legal requirements for critical and important sector entities. The material scope of the NIS 2 Directive is expressed in Article 2(1) read in conjunction with the Annexes to the Directive and Commission Recommendation 2003/361/EC [19]. The scope of the NIS 2 Directive is somewhat fragmented, and a flowchart depicting the scope of the NIS 2 Directive is described in Figure 1 below.

2.2 The Material and Territorial Scope of the GDPR

The material scope of the GDPR is primarily regulated in Articles 1 and 2 of the regulation. According to Article 1, the GDPR regulates the processing of personal data in the EU. Therefore, the two definitions – processing and personal data – are crucial in determining the scope of the GDPR.

Article 4(1) of the GDPR defines personal data as "any information relating to an identified or identifiable natural person [the] ('data subject')". The term "identifiable" is further defined in the same article as the possibility of direct and indirect identification of a natural person, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person.

Processing is defined in the GDPR Article 4(2) as "any operation or sets of operations which is performed on personal data or on sets of personal data". Storing, using, adapting, or altering data is therefore under the scope of the GDPR if the data processed fulfils the definition of personal data.

Regarding the territorial scope, the GDPR applies when a controller processes personal data in the context of the activities of an establishment of a controller or processor established in the Union, irrespective of whether the processing takes place on physical servers, geographically, placed within the Union, according to Article 3 of the GDPR.

2.3 The Common Scope of the NIS 2 Directive and the GDPR

Under which circumstances do both the requirements in the GDPR and the NIS 2 Directive apply? Firstly, the territorial scope of the GDPR requires that the processing of personal data is in the context of "the activities of an establishment of a controller or a processor in the Union", according to Article 3(1) GDPR. The NIS 2 Directive applies, on the other hand, to entities "which provide their

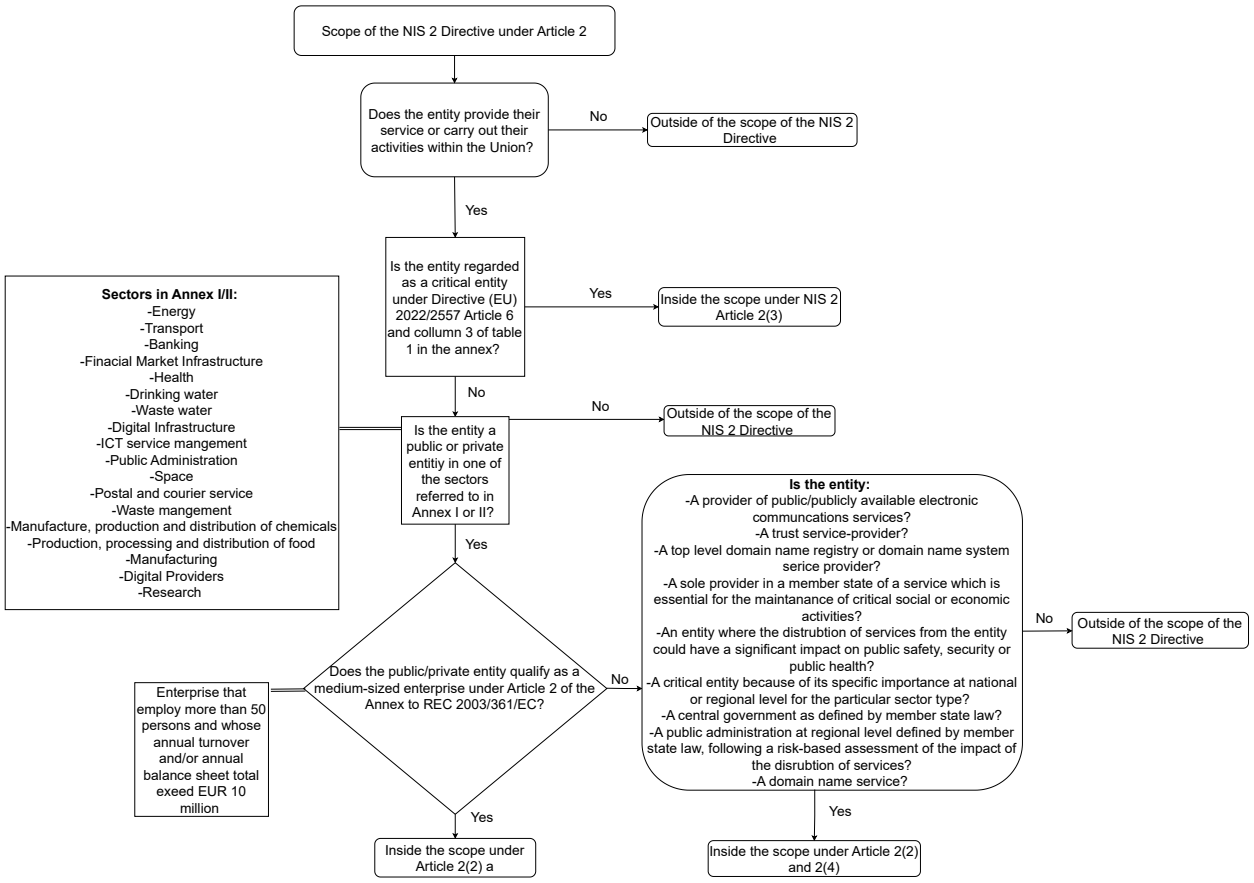

Fig. 1. Flowchart of the scope of the NIS 2 Directive.

services or carry out their activities within the Union", according to Article 2(1) of the NIS 2 Directive. With regard to the European Economic Area (EEA), the EEA relevance of the NIS 2 Directive is currently, as of November 2023, under scrutiny by EEA/EFTA [22].

The first question to consider in order to interpret the common scope of the two legal frameworks is whether these two definitions of the territorial scopes are to be interpreted differently. The territorial scope of the GDPR in Article 3(1) requires that personal data is processed in relation to the "activities" of an establishment of a controller or processor in the EU. The physical processing, e.g., the server capacity, does not need to be situated within the EU, as long as the processing relates to the "activities" of an "establishment" in the EU.

The GDPR might also come into effect under Article 3(2) of the regulation. Article 3(2) extends the scope of the regulation to controllers outside of the Union if the processing is related to the offering of goods and services or monitoring of the behaviour of data subjects in the Union. The relevant assessment with regard to the territorial scope under Article 3(2) is whether data subjects in the Union – regardless of nationality or legal status – are targeted. In this assessment, Recital 23 of the GDPR specifies that the language, currency, and whether the goods and services can be delivered within the member states are relevant factors.

The next question under consideration is whether the wording in the NIS 2 Directive Article 2(1), "provide their services or carry out their activities within the Union" overlaps with the territorial scope of the GDPR established above. The GDPR Article 3(1) and (2) is characterised by its extraterritoriality. However, it is unlikely that entities in sectors of high criticality under the NIS 2 Directive – such as critical sector entities that supply energy or drinking water – do not have a physical presence in an EU member state. Non-physical presence is more conceivable for services such as publicly available communications services and services offering cloud computing, as outlined in Annex 1 Sector 8 of the NIS 2 Directive. In order to get the full picture of the territorial scope of the NIS 2 Directive, the wording of Article 2(1) of the directive needs to be interpreted in line with Recital 113. Recital 113 – concerning the jurisdiction of member states for entities falling under the scope of the directive – presupposes that the entities are established or have a main establishment in one of the EU member states. Therefore, the wording of the NIS 2 Directive Article 2(1) "provide their services or carry out their activities within the Union" must be interpreted as entities with a main establishment in a member state and does not open for an extraterritorial scope as under the GDPR.

Despite the fact that the NIS 2 Directive does not have an extraterritorial scope, the GDPR and the NIS 2 Directive overlap in their material scopes. The NIS 2 Directive and the GDPR share a common scope for controllers in the EU that process personal data, where the controller also enters the scope of the NIS 2 Directive under Article 2 of the directive. This common scope can be illustrated with some examples. For instance, consider a postal carrier established in the EU that employs a mobile application to deliver parcels. The mobile application has a feature that allows the data subjects to track the status of their shipment.

The postal carrier would be considered as controller under the GDPR for the processing of personal data in the application. Additionally, postal and courier services fall under the scope of the NIS 2 Directive, according to the NIS 2 Directive Article 2(1) and Annex II Table 1 point 1) and Directive 97/67/EC Article 2 point (1a). As a result, the controller would be required to comply both with the risk assessments under Article 32 of the GDPR and Article 21 of the NIS 2 Directive.

Another example is a healthcare provider established in the EU that has acquired a new patient journal system. Such a system processes personal data and special categories of personal data under Article 9(1) of the GDPR. The health care provider is the controller for the personal data in the journal system, pursuant to Article 4(7) GDPR. Additionally, healthcare providers are classified as a sector of high criticality under Article 2(1) of the NIS 2 Directive, Annex I Table 1 Sector 5, and Directive 2011/24/EU. These examples demonstrate that controllers under the GDPR may also fall under the scope of the NIS 2 Directive and, as a result, must comply with both rule sets simultaneously.

2.4 NIS 2 and GDPR: Potential Conflicting Requirements

It is essential to keep in mind, despite some overlap in the material scope, that the GDPR and the NIS 2 Directive have distinct backgrounds, contexts, and objectives. The GDPR regulates the processing of personal data in the EU, with the aim of protecting the fundamental right to data protection and ensuring the free flow of personal data across the member states. In contrast, the NIS 2 Directive aims to protect the digital infrastructure itself from cybersecurity incidents and thereby ensure societal protection from cybersecurity attacks. The primary aim of such societal protection is the functioning of the internal market through operational resilience, rather than the protection of the personal data of natural persons processed by the systems.

Do these differences in background and purpose between the GDPR and the NIS 2 Directive result in conflicting requirements? The protection of personal data presupposes adequate cybersecurity measures and proper cyber hygiene within an organisation. However, in certain circumstances, the principles and requirements of the GDPR might have the potential to contradict or conflict with the obligations of critical and important sector entities in the NIS 2 Directive.

According to the NIS 2 Directive Article 26(1), EU member states are required to facilitate the exchange of relevant cybersecurity information among essential and important entities. In the event that such an information-sharing process involves personal data, the information-sharing is also considered processing of personal data under the GDPR. However, Article 25(1) of the NIS 2 Directive stipulates that this information-sharing process is without prejudice to the GDPR.

Nonetheless, the question arises as to which legal basis in the GDPR an information-sharing process for cybersecurity purposes could be based on. Several grounds call for such information-sharing to be based on the GDPR Article

6(1)(f) (legitimate interests). According to Recital 49 of the GDPR, the processing of personal data "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security" is considered as legitimate interests. Similarly, Recital 69 of the NIS 2 Directive highlights that processing personal data for the purposes of network security would be regarded as a legitimate interest under the GDPR. Therefore, the information-sharing in the NIS 2 Directive Article 26(1) could rely on Article 6 (1)(f) as the legal basis and processing of personal data for such a purpose would – to the extent it is strictly necessary and proportionate – be lawful under the GDPR.

Article 6(1)(f) cannot serve as a valid legal basis for the processing of personal data carried out by public authorities in the performance of their tasks, pursuant to the second paragraph of Article 6(1)(f). The NIS 2 Directive also applies to public authorities in high-criticality sectors. In case a public sector controller processes personal data for information-sharing purposes under NIS 2 Article 25(1), Article 6(1)(e) of the GDPR could serve as a valid legal basis. This legal basis could be applied to the processing of personal data when the processing "is necessary for the performance of a task carried out in the public interest", or when the processing of personal data for cybersecurity purposes by the public critical sector authority is regarded as an exercise of official authority. Public sector critical entities processing personal data for cybersecurity and network security purposes could, therefore, rely on Article 6 (1)(e). However, the right to object in Article 21(1) GDPR applies to processing based on both Article 6(1)(e) and (f). As a result, the data subject could potentially object to the processing for cybersecurity purposes, rendering the two legal bases in both Article 6(1)(e) and (f) ineffective. If the obligations under the NIS 2 Directive are interpreted together with Article 32 of the GDPR, Article 6 (1)(c) might provide a valid legal basis for processing. Article 6(1)(c) – a legal obligation to which the controller is subject – may, therefore, be a more efficient legal basis compared to Articles 6 (1)(e) and (f), as the right to object under Article 21 does not apply under Article 6(1)(c), according to Article 21(1) of the GDPR.

Another example of potential conflict between the GDPR and the NIS 2 Directive pertains to cybersecurity audits. In line with Article 29(2) (e) of the NIS 2 Directive, EU member states must equip competent authorities with the ability to request information necessary to conduct audits of the security measures of the essential and important sector entities. One possible consequence of the risk of future audits is that essential entities may store results from cybersecurity incidents in anticipation of forthcoming audits. If such information constitutes personal data, storing it may conflict with the principle of storage limitation in the GDPR, as outlined in Article 5(1)(e). The storage limitation principle requires personal data to be kept only as long as necessary for the purposes it was collected. The assessment of how long it is necessary to store information deemed as personal data may, therefore, differ between the GDPR and the NIS 2 Directive. However, controllers may justify a longer storing period of personal data in such a case based on the provisions of the NIS 2 Directive. It is, nevertheless, important to stress that technical and organisational measures

should be implemented in line with the data protection by design principle set out in Article 25(1) of the GDPR in such situations. For instance, the controller may preemptively store personal data for longer periods if it is pseudonymous or securely stored by other technical methods. By implementing data protection by design principles, data protection risks can be mitigated and, the information necessary for future audits under the NIS 2 Directive could – at the same time – be available.

In accordance with Article 10(2)(d) and (e) of the NIS 2 Directive, National Computer Security Incident Response Teams (CSIRTs) are required to provide dynamic risk and incident analysis, as well as a proactive scanning of the entities' networks and information systems upon request from the entities. Such processes may involve the processing of personal data and, as stated in Recital 25 of the NIS 2 Directive, such scans are in line with the GDPR. However, in such a situation several requirements of the GDPR might not coincide with the purpose of the proactive scan. For instance, in line with Article 15(1)(c) of the GDPR, data subjects have the right to access information on the recipients with whom the controller has shared or disclosed their personal data. According to a judgement by the Court of Justice of the European Union (CJEU) of the 12$^{\text{th}}$ of January 2023 [8], the data subject has the right to get access to the identity and name of the recipient, not just the category of the recipients. The objective of the proactive scan of the network and information system of critical and important entities is to detect any potential security threats in the system. If adversaries are able to access information about their detection through the access right in Article 15 of the GDPR, it may result in a conflict between the legal frameworks and their respective purposes. However, if such a scenario were to occur – where the access right under the GDPR collides with the purpose of the incident scan and analysis under the NIS 2 Directive – it is highly likely that the controller may apply limitations to the access right under member state law in line with Article 23(1) of the GDPR, meaning that the access right under Article 15 would not be fulfilled. Additionally, in case member state law does not have such an exemption, a data subject requesting access under Article 15 must validate their identity for the access right to be fulfilled. Such an identity check may also reduce the risk of the proactive scan under the NIS 2 Directive and the access right under the GDPR colliding in purpose.

In the event of a conflict between the NIS 2 Directive and the GDPR, it is important to determine which legal framework should take precedence. While such a direct conflict would be rare, it is essential to address the antithesis between security and privacy in software system development [14] and decide which norms in the NIS 2 directive or the GDPR should prevail in case of conflict. An important starting point when resolving such a question is that the GDPR is a regulation closely linked to fundamental rights in the Charter, while the NIS 2 is a directive. A conflict of norms between the GDPR and the NIS 2 Directive would, therefore, be a conflict between a regulation with direct effect in the EU and national member state law. In such a scenario with a direct conflict

between the GDPR and the NIS 2 Directive, the requirements in the GDPR would likely take precedence [6,7,9].

On the other hand, it is also important to assess whether some of the requirements in the GDPR and the NIS 2 Directive have the potential for convergence. While the requirements in the two legal frameworks have the potential for legal collision, the primary objective of both frameworks – the protection of systems against cybersecurity incidents and secure processing of personal data – suggests an alignment. The NIS 2 Directive presents opportunities for convergence with the GDPR in situations such as the following examples.

The reporting obligations for critical and important entities in the NIS 2 Directive are harmonised with the reporting obligations for controllers in case of a breach of the security of personal data under the GDPR. Article 32(1) of the NIS 2 Directive establishes that the competent authorities under the Directive may forward a cybersecurity incident reported by an essential or important entity to the national data protection authority in accordance with Article 33 of the GDPR. As a result, essential and important sector entities that experience a cybersecurity incident that also involves a personal data breach are only required to report the incident to one national authority, in line with the single point of contact principle outlined in Article 8 of the NIS 2 Directive.

Considering that a cybersecurity incident may result in a breach of the security of the processing of personal data, essential and important sector entities that process personal data may be subject to fines under both the NIS 2 Directive and the GDPR. However, as stated in Article 32(2) of the NIS 2 Directive, these entities and controllers can only be fined under one of the legal frameworks pursuant to the principle that no legal action could be instituted twice for the same cause of action (ne bis in idem).

2.5 Risk Management in the NIS 2 Directive and the GDPR: Risks to Public Interests vs. Risks to Rights

Are the risks managed under the NIS 2 Directive and Article 32 of the GDPR inherently different? In order to answer this question, the risk management requirements of both the NIS 2 Directive and the GDPR must be analysed.

The risk management measures in the NIS 2 Directive consist of three main pillars: I) Governance, II) Risk-management measures, and III) Reporting obligations. The cybersecurity risk-management measures in the NIS 2 Directive Article 21 shall ensure appropriate and proportionate technical, operational, and organisational measures to manage the risk of cybersecurity incidents. The relevant risks are both risks posed to the security of network and information systems, and risks due to the impact on the recipients of the service, according to Article 21(1) second paragraph. Downtime in a healthcare system may, for instance, pose a risk both to the functioning of that specific system, and also to the healthcare and well-being of patients.

In the assessment of which technical, operational, and organisational measures are appropriate to mitigate identified risks, the state-of-the-art, European and international standards, and the cost of implementation could be taken into

account, according to Article 21(2) of the NIS 2 Directive. In the overall assessment of the proportionality of the risk-management measure, due account should be taken to the entity's exposure to risk, the size of the entity, the likelihood of occurrence and the severity of potential cybersecurity incidents, and the societal and economic impact of cybersecurity incidents, pursuant to Article 21(2).

In line with NIS 2 being a directive and that the member states, therefore, have more autonomy and choice in implementing the requirements in national law, Article 21(2) (a) – (d) lists the minimum requirements for cybersecurity incidents risk-management measures. The measures should have an all-hazard approach and should include policies on risk analysis and information system security, incident handling, and business continuity. The business continuity measures include strategies for backup management, supply chain security, security in the acquisition of network and information systems, policies on the effectiveness of cybersecurity risk-management, cybersecurity hygiene and training, procedures on encryption and cryptography, human resources security, access controls and asset management, and the use of authentication solutions.

Article 24 of the GDPR mandates controllers to pursue the rights and obligations in the regulation through a risk-based approach. The requirements in Article 24 must be interpreted together with Article 32 regarding the security of the processing of personal data and Article 25 regarding data protection by design and by default. The controller, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context, and purposes of the processing of personal data as well as the risk of varying severity and likelihood, must implement appropriate technical and organisational measures to ensure appropriate security of the processing of personal data. Such technical and organisational measures could include pseudonymisation and encryption of personal data. Moreover, the ability to ensure confidentiality, integrity, availability, and resilience in the systems and services, the ability to restore the availability and access to personal data in the event of an incident, and processes for testing, assessing, and evaluating the security of processing.

When assessing risk to the security of the processing of personal data under Article 32 of the GDPR, Recital 76 of the regulation requires that risks are evaluated on the basis of an objective assessment, where it is established whether data processing operations involve a risk or a high risk. The GDPR does not contain a risk assessment methodology for assessing such risks. However, the principle of accountability in Article 5(2) requires that such a risk assessment is systematic and that future audits are possibly conducted from the risk assessment. Several European data protection authorities recommend the use of international standards – such as ISO/IEC 27001 from the International Standardization Organization (ISO) and the International Electrotechnical Commission (IEC) [24] – when risk-assessing under Article 32 of the GDPR [18]. Originally ISO/IEC 27001 is a standard for information security and not specifically data protection.

The main purpose of the GDPR, as expressed in Article 1 of the regulation, is both to protect natural persons with regard to the processing of personal data and to ensure the free movement of personal data within the Union. Natural

persons cannot be efficiently protected with regard to the processing of personal data without efficient cybersecurity measures and risk management of cyber security incidents, as expressed in Article 32 of the GDPR. The risks managed through Articles 32, 24, and 25 of the GDPR are risks both to the security of the processing of personal data and the risks to the rights and freedoms of the data subjects, according to 32(1). The relevant rights for the data subjects are the right to privacy and data protection and the specific rights in Articles 12 to 22 of the GDPR. The fundamental freedoms cover both respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity, according to Recital 4 of the GDPR.

Assessing the risks to the security of a software system in a critical or important sector entity and the risks to the security of personal data processing might initially seem like two similar risk assessments. However, when keeping in mind that the risk assessments under the NIS 2 Directive shall identify and mitigate risks to systems in critical sector entities to reduce negative societal effects and that the risk assessments under the GDPR shall identify and mitigate risks of adverse impact on the rights and fundamental freedoms of data subjects, the assessments seem different. Firstly, the public interests pursued in the NIS 2 Directive and the individual rights and freedoms pursued under the GDPR are inherently distinctive. Secondly, a risk to an information system and a risk to a right are also unique in relation to the risk assessment methodology typically applied [25]. While a risk to the security of a system could be measured into the likelihood and severance of the risk materializing, a risk to a right is more value-embodied and harder to quantify in metrics.

To conclude, security aspects are a crucial part of an assessment of the security of processing personal data under the GDPR. However, the risk assessments under the NIS 2 Directive and the GDPR have different purposes and are not coinciding.

3 Cybersecurity in AI systems in the AIA

As stated in the introduction, a specific AI regulation is emerging in the EU. The following section will analyse whether there are differences in the concepts of cybersecurity across the NIS 2 Directive and the proposed AIA. The references to specific articles in the AIA refer to the Commission's 2021 proposal.

"Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI-specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the

risks, suitable measures should therefore be taken by the providers of high-risk AI systems." [4].

The cited excerpt from the Recital of the proposed AIA highlights the critical role and importance of cybersecurity in AI systems. AI systems might both, due to their internal opaqueness, pose risks to cybersecurity, but AI systems also show significant potential to be used to improve the cybersecurity of systems and networks [10]. Recitals 51 and 89 of the NIS 2 Directive emphasise that both the EU member states and the critical sector entities should pursue the use of cybersecurity-enhancing technologies, such as AI and ML systems to enhance their capabilities and the security of networks and information systems.

What is the role of cybersecurity in the proposed AIA and how might the future interplay between the AIA and the NIS 2 Directive take form? The proposed AIA regulates AI in the EU through a risk-based approach where AI systems are categorised after their potential impact on fundamental rights and harms to the health and safety of natural persons. The categorisations range from prohibited AI systems, high-risk AI systems, and minimal-risk AI systems. The most substantial requirements are imposed on high-risk AI systems. Such systems include the management and operation of critical infrastructures, according to Annex III of the act. Annex III Section 2 to the AIA lists AI systems applied in the management of road traffic, and supply of water, gas, heating, and electricity as high-risk AI systems as their failure might put at risk the life and health of persons at a large scale. The reference to critical infrastructure in the AIA is not coherent with the concept of critical entities in the NIS 2 Directive. The lack of a cross-reference in the two legislations could lead to an inconsistent interpretation of critical entities and infrastructures across the NIS 2 Directive and the AIA.

The interplay between the NIS 2 Directive and the AIA is best illustrated by the use of an example. Suppose that a road traffic authority makes use of a video-based AI system to manage traffic in a city region. Such a road traffic entity must comply with the requirements for entities in the sector of high criticality pursuant to the NIS 2 Directive Article 2(1) and Annex 1 Section 2(d). Furthermore, if an AI system is used in such a critical entity the proposed AIA comes into effect – assuming that the AIA has entered into force in the EU.

First of all, the requirements in the AIA differ between providers and users of AI systems. As a starting point, suppose that the public road traffic agency, a critical entity under the NIS 2 Directive, is the provider of the AI system. A provider of an AI system is defined in Article 3(1) of the AIA as "a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view of placing it on the market or putting in into service under its own name or trademark (...)". If the public road traffic management agency internally develops an AI system for road traffic management, it will fulfil the definition of provider in the AIA.

The requirements for providers of high-risk AI systems are outlined in the AIA Articles 16 and 17, which include obligations for a risk-management system, quality criteria for training, validation and testing the AI models, technical documentation, record-keeping, transparency obligations, human oversight, and re-

quirements for accuracy, robustness, and cybersecurity. The providers must also comply with relevant conformity assessment procedures, comply with a quality management system, and meet various reporting, notification, and marking requirements. Among the AIA provisions, Article 15(4) has significant similarities with the NIS 2 Directive, requiring that high-risk AI systems shall "be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities".

Now suppose that the public road traffic management entity is a user and not the provider of a high-risk AI system. A user of an AI system is defined in Article 3(4) of the AIA as "any natural or legal person, public authority, agency or other body using an AI system under its authority (...)". The requirements for users of high-risk AI systems, pursuant to Article 28(2-5) AIA, are that the users shall use the systems in accordance with the instructions, the user shall ensure that the input data is relevant for the application of the high-risk AI system, and the users shall monitor the operation of the high-risk AI system based on the instructions of use.

The examination of the interplay between the cybersecurity provisions of the AIA and the NIS 2 Directive requires an interpretation of the different purposes of the two legal frameworks. A high-risk AI system – for instance, the road traffic management system – is high-risk due to the inherent risk such an AI system may pose to the health and safety of natural persons. At the same time road traffic management is regarded as a critical sector entity under the NIS 2 Directive due to the importance such an entity has at a societal level. The cybersecurity requirements in the AIA, therefore, primarily aim to protect the natural person's health, safety, and fundamental rights from harm and interference. The cybersecurity requirements in the NIS 2 Directive first and foremost aim to increase cyber resilience and thereby reduce the negative societal impact a cyber incident could have on society and the economy in the internal market.

Even though the two different legal frameworks have different objectives, backgrounds and scopes, several positive synergies could be made by working together and including, for instance, aspects of the risk-management process in the NIS 2 Directive in the risk- and quality management under the AIA and vice versa in cases where both the AIA and the NIS 2 Directive comes into effect. If aspects of the risk of cyber incidents are included in the quality and risk management of AI systems, there are reasons to believe that the overall security, trust, confidence, and resilience of AI systems might increase.

4 Discussion

In the last decade, there has been a surge in EU regulation concerning our ever-evolving digital infrastructures. This includes the GDPR, the NIS 2 Directive, and the AIA and regulations not expressly discussed above as the Data Governance Act [15], the Digital Markets Act [16], and the Digital Service Act [17]. All these regulations have specific objectives and aims, but the surge of regulations has made compliance in software system development a complex and fragmented

task. One common denominator of the regulations that are part of the Digital Single Market [26] in the EU is their focus on compliance with corresponding sanctions for non-compliance.

Hence, we argue for considering compliance issues early and throughout the software development process and thereby include compliance issues in the requirement specification, design, implementation, testing, and deployment phases. As a consequence, software developers need to be competent in the frameworks and regulations. Alternatively, relevant legal expertise can complement the technically skilled personnel. One potential for future research is to assess all of these different regulations through a holistic approach where compliance assessments are regarded as non-functional properties in software systems entering the European market. The difference between assessing risks to public interests and risks to rights would entail that the risk assessments under the NIS 2 Directive, the GDPR, and the AIA are conducted individually but that the internal teams that conduct such assessments work together in order to achieve synergetic effects.

The different risk assessments in the NIS 2 Directive, the GDPR, and the AIA call for assessments of both technical and organisational risks. While a lot of focus has been put on risk management processes as part of compliance assessments, in the end, it is the technical infrastructure that protects personal data from breaches and the software systems from cyber incidents. Compliance with all of these regulations should, thus, not only be regarded as a process to become paper-compliant, but as a process to protect natural persons from personal data breaches, to protect our digital economies from the negative impact of cyber-attacks, and to safeguard persons from harmful AI systems. In such a legal/technical compliance process important aspects include cross- and interdisciplinary cooperation, assessing compliance ex-ante, and including compliance aspects as non-functional properties in the software systems development processes. Such a development approach is in line with the original data protection by design approach in Article 25 GDPR, an approach where risks are assessed and identified and technical and organisational measures are introduced in order to mitigate identified risks.

Based on the legal analysis of the NIS 2 Directive, the GDPR, and the proposed AIA, the following recommendations could be made for software developers and analysts developing software systems under the scope of these existing and forthcoming rule sets. Firstly, if a requirement in national member state law implementing the NIS 2 Directive is in direct conflict with the GDPR, the GDPR will, most likely, prevail. Moreover, as a general finding, the risk management process under the NIS 2 Directive and the GDPR are separate assessments. However, positive synergies could be made through close cooperation between the teams conducting such risk assessments. It is also important to note that the NIS 2 Directive and the proposed AIA have a converging scope if critical sector entities apply high-risk AI systems. When assessing the risk management of the NIS 2 Directive and the AIA, it is important to have in mind the different objectives of the two frameworks. The AIA should, primarily, protect natural persons from harm from the AI system, while the NIS 2 Directive should pro-

tect the infrastructure itself from cyber incidents. A general conclusion is that the surge of EU regulation regarding personal data protection, digital markets, cybersecurity, and AI should be assessed holistically to get positive synergistic effects from the different risk management processes in the different legal frameworks. Ideally, such a holistic process should be made as early as possible in the software system development process.

References

1. Lawrence Chung, Brian A Nixon, Eric Yu and John Mylopoulos, Non-functional requirements in software engineering, Springer Science & Business Media 2012 (5).
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending regulation (EU) NO 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80. See NIS 2 Article 41(1) for the date of entry into force of the directive.
4. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts COM/2022/206 final. Recital 51.
5. European Commission, Regulatory framework proposal on Artificial Intelligence. Available: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai last accessed: 22.11.2023.
6. Livinus Obiora Nweke and Stephen Wolthusen. Legal issues related to cyber threat information sharing among private entities for critical infrastructure protection. 2020 12th International Conference on Cyber Conflict (CyCon). Vol. 1300. IEEE, 2020. DOI: 10.23919/CyCon49761.2020.9131721.
7. Richard Borden et. al. Threat Information Sharing Under GDPR available: https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2019/spring/threat-information-sharing-under-gdpr/ last accessed: 22.11.2023.
8. Case C-154/21 *Österreichische Post* ECLI:EU:C:2023:3 (Grand Chamber).
9. Dimitra Markopoulou et. al. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6, 2019, 105336. DOI: 10.1016/j.clsr.2019.06.007.
10. Iqbal H. Sarker et. al. , AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN COMPUT. SCI. 2, 173 (2021). DOI: 10.1007/s42979-021-00557-0.
11. Martin Horák et. al. GDPR compliance in cybersecurity software: a case study of DPIA in information sharing platform. Proceedings of the 14th international conference on availability, reliability and security. 2019. DOI: 10.1145/3339252.3340516.
12. Harsha Perera et. al. Towards integrating human values into software: Mapping principles and rights of GDPR to values." 2019 IEEE 27th international requirements engineering conference (RE). IEEE, 2019. DOI: 10.1109/RE.2019.00053.
13. Abdel-Jaouad Aberkane, Geert Poels and Seppe Vanden Broucke. Exploring Automated GDPR-Compliance in Requirements Engineering: A Systematic Mapping Study. IEEE Access 9 (2021): 66542-66559. Doi: 10.1109/ACCESS.2021.3076921.

14. Sue Conger and Brett JL Landry. The intersection of privacy and security. (2009). All Sprouts Content. 243.
15. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1.
16. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L 265/1.
17. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277/1.
18. Datatilsynet, Vedtak om pålegg-PostNord AS, 20/02144-16. Information Commissioner's Office (ICO), Security requirements. Danish Data Protection Authority, passende tekniske og organisatoriske foranstaltninger.
19. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC) [2003] OJ L 124/36.
20. Andrey Y. Iskhakov et. al. Adaptive Authentication System Based on Unsupervised Learning for Web-Oriented Platforms. In Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023 (pp. 507-522). Springer Nature Singapore.
21. Govert Valkenburg, Privacy Versus Security: Problems and Possibilities for the Trade-Off Model, Reforming European Data Protection Law. DOI: 10.1007/978-94-017-9385-8_10.
22. EFTA, Directive (EU) 2022/2555. Available: https://www.efta.int/eea-lex/32022L2555. Last accessed: 22.11.2023.
23. EDPB, Guidelines 3/2018 on the territorial scope of the GDPR Version 2.1 page 4. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en. Last accessed: 22.11.2023.
24. ISO, ISO/IEC 27001 and related standards. Available: https://www.iso.org/isoiec-27001-information-security.html. Last accessed: 22.11.2023.
25. Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, A risk to a right? Beyond data protection risk assessments, Computer Law & Security Review, 32:2, https://doi.org/10.1016/j.clsr.2015.12.017.
26. European Concil, Digital Single Market, available: https://www.consilium.europa.eu/en/policies/digital-single-market/. Last accessed: 24.11.2023.