THE CURRENT AND DEVELOPING REGULATORY FRAMEWORK OF INFORMATION SECURITY IN THE EU AND THE REPUBLIC OF CROATIA

Review article

UDK 34:004.3/.4(497.5:4 EU)
340.5

Received: November 2, 2023

Tihomir Katulić*
Hrvoje Lisičar**

Information security involves ensuring the reliable, confidential and trustworthy operation of information systems and preserving the availability and reliability of data. Its framework and content are increasingly regulated by law. Research consistently shows that the number of attacks on information systems as well as data breaches is rising. Information security practices are no longer just a matter of recognised industrial self-regulation standards but are instead increasingly the focus of legislators in the European Union as well as in comparative law. In the last five years, the regulation of information security in the European Union has undergone significant changes and expansion through numerous regulations, directives and legislative proposals that are still under development. This paper provides an overview and basic analysis of the current positive legal framework for information security in the European Union and the Republic of Croatia from substantive and institutional aspects. Specific regulations containing provisions in the field of information security are listed chronologically, and de lege ferenda proposals are also considered.

Keywords: information security, NIS Directive, NIS2, Cybersecurity Act, GDPR

1. INTRODUCTION

Information security has become an integral part of our digital society practices. It involves protecting information from unauthorised access, disclosure, disruption, modification, or destruction, thus ensuring confidentiality, integrity, and availability.[1]

In the European Union (EU), the regulation of information security has emerged as a critical part of its broader digital policy framework. The reasons range from obvious requirements of transition into the digital, information society, such as the growing reliance on digital platforms and massive electronic data processing technologies and services. In turn, this requires a trustworthy and safe environment to ensure the protection of sensitive and personal data.

* Tihomir Katulić, PhD, Associate Professor at the Department of Information Technology Law and Informatics, University of Zagreb Faculty of Law
** Hrvoje Lisičar, PhD, Associate Professor at the Department of Information Technology Law and Informatics, University of Zagreb Faculty of Law
[1] S. Samonas, "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security", Journal of Information System Security, Volume 10, Number 3, 2014, pp. 21-45.

According to research on the nature and trends of cybercrime, which are periodically conducted by EU agencies such as Europol and ENISA,[2] one of the fundamental characteristics of cybercrime is its positive correlation with the availability of information technologies and the ease of their use.

Research consistently shows that the number of attacks on information systems as well as data breaches is rising.[3] Cyberattacks, data breaches, and other security incidents can lead to significant economic and societal harm, disrupting essential services, eroding trust in digital platforms, and potentially infringing privacy and data protection rights. In addition to complex attacks that require perpetrators to have a high level of technical knowledge, mass attacks by perpetrators with a relatively low level of technical knowledge, as well as attacks perpetrated using computers and other devices connected to the internet without the knowledge of their owners or authorised users, are becoming increasingly common. In recent years, according to ENISA data, there has been a noticeable increase in attacks through the use of malicious programs (malware), particularly a specific type of malicious program – ransomware – that is, a malicious program that, like computer viruses, infects the information system and then encrypts user data with strong encryption algorithms, making them unreadable by system users. According to other researchers, damage from the use of this category of malicious programs alone exceeds on the global level EUR 5 billion. At the same time, this current form of cybercrime represents only a small share of total activity. According to some estimates, the total damage to the world economy caused by cybercrime exceeds USD 3,000 billion dollars.[4]

In general, it can be concluded that the proliferation of information technologies, especially software and services intended for communication and data exchange via the internet, has indirectly strongly contributed to the development of a new generation of sophisticated malicious programs that can be used for precise and efficient attacks on data and information systems.[5] Thus, according to data from the European Commission, over 80 percent of European companies suffered at least one attack on information systems in the previous year and the total number of attacks according to the same report increased by almost 40 percent compared to the year before.[6] The scale of cybercrime, especially the so-called *dark figure of cybercrime*, the number of committed but

[2] ENISA – European Network and Information Security Agency, www.enisa.europa.eu.
[3] The ENISA Threat Landscape is a yearly assessment of the state of the cybersecurity threat landscape. The report presents and analyses recognised high risks, significant trends in threats, threat actors, and attack methods, along with impact and motive analysis. It also lists recommended mitigation strategies. The report is available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[4] According to Fortinet Cybersecurity Statistics 2022, available at https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics. See CISCO and Cybersecurity Ventures. Report available at: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion.
[5] M.G. Porcedda, "Patching the Patchwork: Appraising the EU Regulatory Framework on Cyber Security Breaches", Computer Law & Security Review, Vol. 34(5) 2018, p.1077.
[6] ISACA report "State of Cybersecurity", available at https://www.isaca.org/go/state-of-cybersecurity-2021.

undiscovered or unreported incidents, represents a significant problem for societies in transition to a post-industrial, information society.[7]

Information security involves ensuring the reliable, confidential and trustworthy operation of information systems and preserving the availability and reliability of data. Its framework and content are increasingly regulated by law. In this sense, modern legislation considers different approaches to the regulation of information security, i.e. ensuring the confidentiality, integrity and availability of information systems and data as its fundamental paradigm. There is significant literature on the subject of the governance of information security, as well as what constitutes information security governance.[8]

European lawmakers have repeatedly tried to lay the foundations of the European information security protection system through normative intervention. The results of these efforts have been somewhat incomplete and deficient. The cause of this should be sought in the legal basis of information security regulation, the connection of this topic with the broader topic of national security, and not within the competence of the European legislators, and in the selected instruments of the implementation of the *acquis* in the legislation of the Member States.[9]

It is clear, from a practical point of view, that without adequate cooperation of the Member States of the Union, regularly across national borders, among all the participants participating in the services of the information society, the goal of having effective measures to prevent future incidents and attacks may be unreachable.

In this paper, we will refer to and present a series of regulations that make up the European legal *acquis* in the field of information security. Previously, where the Directive on the protection of network and information systems (the so-called NIS Directive), adopted by the European Parliament in July 2016, used to take centre stage, now there are several Directives and Regulations that not only define the scope of information security provisions, the institutional framework at the European and Member State level, but also the specific requirements in sectors of public and private institutions and enterprises. This proverbial *legislative tsunami* of sorts is a reflection of the Commission's awareness of the need to coordinate information security activities in the territory of the Member States.

Of course, legislative efforts are not the only method of political action. For the purpose of improving the overall state of European information security, significant funds are being earmarked for research and innovation programmes in the field of information security,

---

[7] D. Dragičević, N. Gumzej, M. Jurić, T. Katulić, H. Lisičar, "Pravna informatika i pravo informacijskih tehnologija", Narodne Novine, Zagreb, 2015, p. 171.

[8] S. AlGhamdi, W.K. Than, E. Vlahu-Gjorgievska, "Information Security Governance Challenges and Critical Success Factors: Systematic Review", Computers&Security, Vol. 99, 2020.

[9] D. Markopoulou, V. Papakonstantinou, P. de Hert, "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation", Computer Law & Security Review, Vol. 35(6), 2019.

in order to encourage European companies towards a higher level of activity on the market of information security products and services, where the Union lags significantly behind the USA and East Asian countries. The EU has also adopted several general policy documents, such as the European Cybersecurity Strategy, the Digital Single Market Strategy, and the European Agenda on Security.[10]

These documents emphasise the need for the Union to remain a globally recognised factor in the field of cyber security and as such to continue to protect the rights of European citizens and European companies in cyber space from various abuses, regardless of whether they are ordinary cybercrime, organised crime, or cyber warfare operations intended to gain access to the information systems of European companies and institutions or to sabotage European information resources, services and data.

New trends in the development of information and communication technologies, especially the *Internet of Things*, *Big Data*, cryptocurrencies and microtransactions, smart materials, machine learning and work on artificial intelligence hold great promise. The complete digital transformation of business (digital transformation) requires that the issue of cyber and general information security becomes an integral part of European policies in all relevant areas.

2. BASIC CONCEPTS OF THE REGULATION OF INFORMATION SECURITY

Information security can be seen as a set of strategies for managing procedures, tools and establishing a security policy to prevent, detect and record threats to (typically digital) data. The International Standards Organization (ISO) 27000:2009 standard defines information security as preserving the confidentiality, integrity and availability of information.[11] The international organisation ISACA (the Information Systems Audit and Control Association) defines information security as the activity of ensuring access to precise and complete information (integrity) by only authorised users (confidentiality) at the moment when the information is needed (availability).

Some authors associate information security with risk management, so their definition of information security implies that it is a risk management method whose task is to manage the cost of the risk that information represents for a business activity.[12] Others define information security as the activity of protecting (confidentiality) information and minimising the risk of exposing information to unauthorised persons. [13] In any case, it can be concluded that information security is actually the name for a broad multidisciplinary

[10] Available at: https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.
[11] ISO 27001 standard, 5th edition 2018, p. 4, available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
[12] B. Blakley, E. Mcdermott, D. Geer, "Information Security Is Information Risk Management", Proceedings of the Workshop on New Security Paradigms, 2001, p. 97.
[13] H.S. Venter, J.P. Eloff,. "A Taxonomy for Information Security Technologies", Computers & Security, Vol. 22(4), 2003, pp. 299-307.

field that includes the development and use of a wide variety of security mechanisms (technical, organisational, legal, etc.) in order to protect information and information systems from various threats inside and outside the organisation and system. As we increasingly accept and use information security in our daily work, the concept of information security is increasingly becoming an integral part of various aspects of the information society.

The use of information technologies entails exposure to various dangers. Any system we use to access data, collect data or process it can potentially become a victim of an attack. Common to all the above definitions is the need to protect data and systems from attacks by those who would like to misuse them. In the literature, the question arises about when we are really safe, that is, when we have ensured an adequate level of security.[14] It is not possible to give an unequivocal answer to this issue. The complexity and sophistication of information systems imply a potentially high number of vectors (directions) of attacks on the system, from attacks at some level of the network base, through the exploitation of vulnerabilities in the operating system or the hardware of the information system itself, to attacks at the local or internet application level, etc. One of the ways to approach the problem stems from the so-called CIA paradigm, that is, the concept of ensuring confidentiality, integrity and availability of data (confidentiality, integrity and availability).[15]

Confidentiality as part of the CIA triad represents a concept that resembles, but is not identical to, privacy. It is the ability to protect data from unauthorised access by persons who do not have permission to access that data. Confidentiality is an integral part of the concept of privacy, but privacy represents a broader concept in terms of content. How can data confidentiality be violated? A hacker who intercepts a client's communication with a bank or other financial institution, a user who loses a mobile phone or other electronic device which is then accessed by an unauthorised finder, or simply unauthorised access to documents marked confidential by a person who does not have a legal or contractual basis for accessing the data contained in them are simple and everyday examples of data confidentiality violations.

Data integrity refers to the ability to preserve data in its original form without the possibility of unwanted or unauthorised changes that could lead to data deletion or change. In order to ensure the integrity of the data, it is necessary to have not only mechanisms to prevent integrity violations, but also data recovery mechanisms, such as exist, for example, in the file systems of modern operating systems.

Finally, the last aspect is availability, that is, the ability to access data as needed, at the moment when there is a need for it. The lack of availability can occur due to problems in the operation of the information system, its operating system or applications, problems

[14] J. Andress, *The Basics of Information Security*: *Understanding the Fundamentals of InfoSec in Theory and Practice*, Elsevier, 2011, p. 3.
[15] Ibid, p. 4.

with the supply of electricity, a network attack or the compromise of individual parts of the information system, etc. The increasingly frequent denial of service attacks are typical examples of external attacks on the availability of data and information systems.

3. DEVELOPING THE EU LEGAL FRAMEWORK OF INFORMATION SECURITY

One of the goals of this paper is to provide an overview of key European documents that contain important measures for raising the European and national level of information security. Since the early 1990s, the European legislator has repeatedly tried to regulate the obligations of Member States in terms of maintaining an adequate level of information security, with variable success.

These efforts especially intensified in the previous decade. The European Information Security Strategy was adopted in 2013. Its main task was to strategically determine the objectives of the European Commission in the field of information security protection and to ensure the adequate resilience of the Union and Member States' systems to the growing threat of cyberattacks and cybercrime.[16]

The Strategy outlines as its basic goals:

- activities in the field of strengthening resistance to cyberattacks;
- the fight against increasingly widespread cybercrime;
- the development of a common European defence policy in cyberspace;
- the development of industrial and technological resources for cyber security;
- the development of a coherent common international policy for the regulation of cyberspace on the territory of the EU, which would include fundamental European values.[17]

Following the adoption of the Strategy, the European Commission in 2015 adopted the European Security Agenda for the period from 2015 to 2020, aware that the seemingly unstoppable rise of cybercrime demands a coordinated response by Member States.

The Agenda proposed that Member States increase their efforts in the following areas of activity:

[16] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, adopted on 7 December 2013, available at: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
[17] Ibid, p. 4

- implementation of proposed policies in the field of cyber security;
- protection against attacks on information systems;
- the fight against various forms of fraud and counterfeiting, especially the counterfeiting of new forms of electronic payment and financial instruments;
- the facilitation of cross-border cooperation in the field of criminal proceedings and investigations against perpetrators of cybercrime, especially problems in the field of jurisdiction and access to evidence, etc.

In addition to the above-mentioned documents, the European Commission also adopted the Digital Single Market Strategy[18] in the same year, an umbrella document whose task is to stimulate European competitiveness and finally unify the fragmented market in the field of digital content distribution. Additionally, the goal of the Strategy is to facilitate the distribution and development of services for the common market for European entrepreneurs and take advantage of all the benefits of the digital transformation of business and to ensure an adequate environment for the development of a network infrastructure and new globally competitive services.[19]

4. THE FIRST NIS DIRECTIVE AND THE CYBERSECURITY ACT

In 2016, after several years in development, the Network and Information Security (NIS) Directive was adopted.[20] As the rise in the number of information security incidents was continuing, the Commission was moved to adopt measures to help protect the information security of Member States, organisations and enterprises in the European market from further information security incidents.

The NIS Directive was the first general EU legal norm unifying information security rules and obligations for Member States, especially considering the obligatory institutional framework required to foster Member State cooperation and incident response. The main goal of the Directive was to ensure a higher level of information security among the Member States through several areas of activity:

- achieving a higher level of competence in the field of cyber security at national levels;
- achieving higher levels of cooperation at the level of the Union;

[18] Digital Single Market, https://ec.europa.eu/priorities/digital-single-market_en.
[19] Ibid, p 2 *et infra*.
[20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, L 194/1 19.7.2016, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148.

- establishing the obligation to manage risks and the obligation to report incidents for providers of digital services, especially of different categories of essential services;

- regulating other obligations of providers of key and digital services.

The NIS Directive called for the adoption of a culture of risk management, stating that it is necessary to adopt adequate risk assessment and security measures appropriate to information security risks in addition to those that are required by law and through voluntary industry practices based on increased awareness of the risks. Operators of so-called essential services in particular had to take the necessary actions and report grave situations to the appropriate national authorities.[21] The Directive introduced common criteria to identify operators of essential and digital services – private businesses or public entities with an increasingly important role for Member State economies – in sectors defined by the Directive as energy (transport and distribution of electricity, oil, gas, etc.), transport (air, rail, maritime and river, and road transport), the banking and financial market infrastructure, healthcare, water (supply and distribution) and the digital communication infrastructure (internet exchange points, domain name system service providers, top level domain name registries, etc).[22] The NIS Directive also defines digital services as information society services – services normally provided for remuneration, at a distance, by electronic means and at the individual request of the recipient.

Like the General Data Protection Regulation, which introduces the concepts of information security and risk assessment into the personal data protection system, the NIS Directive uses the concept of risk management to ensure that incidents that may have serious consequences for the integrity of the services provided are monitored and processed. For adequate risk management and the fulfilment of the obligation to report incidents for key service providers and digital service providers, the first step is to determine which services are essential and which are digital services, and then what exactly can be expected from companies and other entities that provide such services on the common market. According to the provisions of the Directive, providers of essential services are private law bodies (various commercial companies) and public authorities that play an important role in modern society and the economy.

Following the adoption of the NIS Directive, in the *vacatio legis* period of two years (Art. 25 of the original NIS), the Member States started to transpose its provisions into their national legal systems. The NIS transposition was quite diverse, with some Member States transposing the Directive almost literally into a new national law, such as the Croatian Act on Cybersecurity of Operators of Essential Services and Digital Service Providers of 2018,

[21] T. Katulić, "Transposition of the EU Network and Information Security Directive into National Law," 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018, pp. 1143-1148, doi: 10.23919/MIPRO.2018.8400208.
[22] Ibid, p. 5.

while others (for example Finland or the Czech Republic) opted for the adaptation of (a large number of) existing laws in line with the provisions of the NIS Directive.

In 2019, the EU adopted its first information security Regulation, the Cybersecurity Act, replacing an earlier ENISA Regulation from 2013.[23] The EU adopted the Cybersecurity Act as a legislative measure intended to help deal with an increasing number and complexity of cyber threats that threatened European public and private organisation information systems. Another goal of the Regulation was to enhance overall cyber resilience and response across the Member States.

The Regulation expanded ENISA's mandate to become a permanent EU agency with increased resources and new tasks to support Member States in tackling cybersecurity threats and attacks. It also introduced an EU-wide cybersecurity certification framework for information and communication technology (ICT) products, services, and processes designed to ensure that certified products across the EU meet consistent security standards, thus reducing fragmentation and increasing trust.

One of the main reasons why the EU legislators chose the form of a Regulation for this purpose was to ensure a higher level of coordination, information sharing, and collaboration between Member States. Directly applicable law without the need for national transposition and interpretation would work towards enhancing the collective ability of the EU to respond to major cross-border cybersecurity incidents and crises. By introducing a common certification framework, the Cybersecurity Act aimed to further promote the Digital Single Market, promoting the free movement of digital products and services across the EU.

4.1. From the NIS to the NIS2

In November 2022, the European Parliament approved the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).[24] The new Directive, at the time this paper was being prepared, in transposition into the legal systems of the Member States, repeals the original NIS Directive on the security of network and information systems and aims to further develop the common EU rules on the security of network and information systems and help increase the level of cyber resilience required of critical public and private sectors, and the EU as a whole. The original NIS Directive, as the first cybersecurity piece of legislation in the EU, was the first instrument aimed at enhancing the Union's network and information system's resistance

[23] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

[24] 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) (Text with EEA relevance).

to increased cybersecurity risks and the rapid rise of related incidents. Following its adoption, the NIS Directive exhibited certain shortcomings in the face of accelerated transition into an information society environment.

While the Commission conducted thorough stakeholder engagement to analyse the effects and shortcomings of the NIS Directive, certain concerns became apparent. In spite of the transposition of the NIS Directive, the Member States indicated an insufficient level of cyber resilience of organisations operating in the EU, inconsistent results across the Member States and sectors, a lack of common understanding of the main cybersecurity threats and challenges, and a lack of joint crisis response. As a result, and in an effort to address the growing threats brought on by digitalisation and interconnectedness, the Commission proposed a revised set of rules to strengthen the Union's cyber resilience.

The new Directive provides measures to further develop cybersecurity in the EU, building on the foundations that were the basis of the NIS1 Directive, requiring Member States:

- to adopt a national cybersecurity strategy;[25]
- designate computer security incident response teams (CSIRTs);[26]
- designate a competent national cybersecurity authority:[27]
- designate a single point of contact;[28]
- establish an NIS cooperation group and CSIRT network;[29]
- provide obligations for an extended number of critical sectors such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure;
- regulate infringements entailing a personal data breach.[30]

Service providers in sectors identified by the Member States as essential services operators are required to regularly assess the state of cybersecurity of their information systems through mandated risk assessment and to apply appropriate and proportionate security measures.[31]

[25] Ibid, Art. 7 of the NIS2 Directive.
[26] Ibid, Art. 10.
[27] Ibid, Art. 8, para 1.
[28] Ibid, Art. 8.
[29] Ibid, Art. 10.
[30] Ibid, Art. 35.
[31] Chapter IV of the NIS2.

The Directive further regulates the obligation of such providers to notify competent authorities of information security incidents.[32]

5. INFORMATION SECURITY RELATED PROVISIONS IN THE GENERAL DATA PROTECTION REGULATION

The number of regulations in the European Union (EU) that include information security provisions has grown dramatically over time. Several important factors, including the expanding digital economy, the frequency and sophistication of cyberthreats, the need for data protection, and the goal of establishing a unified digital single market, have an impact on this trend. The first, and perhaps most important, factor is that the global economy has mostly transitioned to the digital sphere. The internet and digital technology have shaped everything from business and communication to public services and entertainment, becoming fundamental components of the European economy. Large amounts of data are created, stored, and communicated online as a result of this reliance on digital technology. The security of these data and the systems that handle them is now of the greatest concern.

Furthermore, a major problem is posed by the expansion of cyberthreats both in scope and complexity. Cyberattacks and security lapses can seriously disrupt vital infrastructure, erode public trust, compromise personal data, and result in significant financial loss. They present a global issue since they are not limited by national boundaries. In order to fight this, the EU has created legislation to encourage effective cybersecurity procedures and collaboration among Member States. The next argument relates to the EU's fundamental rights of privacy and data protection. The EU places high priority on individuals' right to privacy and data protection, and in order to protect these rights, information security is of crucial value. Personal data might be compromised without sufficient protections, resulting in data breaches. Laws like the General Data Protection Regulation (GDPR)[33] highlight the EU's dedication to protecting personal data with strict security requirements.

The EU is also working to create a true digital single market where people, goods, and capital can move freely and where people and businesses can easily access and participate in online activities while maintaining high standards of consumer and personal data protection. Even though the Regulation itself mentions only once the term "information security", it is nonetheless abundantly clear that recognised information security practices present a framework for ensuring accountability in personal data processing.[34]

---

[32] Art. 23.

[33] 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), OJ L 119/1.

[34] Recital 49 GDPR.

In general, the provisions of the General Data Protection Regulation pertaining to information security aim to accomplish a number of crucial goals to facilitate data controllers' accountability, a key principle of personal data processing that requires the data controller to be able to demonstrate compliance with the regulations governing personal data processing. Data controllers are liable for personal data breaches – breaches of security that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of personal data, unauthorised access to personal data, or other unauthorised transmission, storage or processing of personal data, and thus have the obligation to ensure that proper security controls are in place to prove safe and secure personal data processing.

Starting with the general data protection principles in Article 5 GDPR, the Regulation systematically introduces information security principles and practices as a compliance mechanism to ensure secure processing and protection of data subject rights. Article 5, for example, as one of the data protection principles, defines the principle of integrity and confidentiality – well-known components of the CIA triad of information security. Further, in Chapter IV, the Regulation provides obligations for the data controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed safely and securely.

For example, Article 24 mandates the implementation of appropriate data protection policies and regular review and updating of technical and organisational measures where necessary. The provisions are accompanied by several recitals that establish the liability of the data controller for the safety and security of processing conducted by the controller or on the controller's behalf, an obligation to implement appropriate and effective measures and ability to demonstrate that the controller is performing processing in compliance with the Regulation.[35]

According to Article 25, the data controller must take organisational and technological steps, such as pseudonymisation, to apply data protection principles like data minimisation and incorporate them into the processing activities. Data controllers should design new programmes, services, and goods based on the processing of personal data with data processing principles in mind from the outset. To ensure what the Regulation refers to as data protection by design and by default, the controller should only process personal data that is essential for the given purpose of processing, taking into account the volume, scope, duration, and accessibility of the data.[36]

[35] Art. 24 GDPR.
[36] Ibid, Art. 25.

The relationship between data controllers and processors is another important topic that the Regulation addresses. The capacity of the controller to realistically impose data protection duties, including information security requirements and procedures on organisations performing the processing job on the controller's behalf has already been scrutinised with regard to this relationship. Because of these concerns, Article 28 GDPR now specifically outlines the rules governing how data controllers and processors should interact. The processor receives personal data from the data controller and follows the controller's specific instructions. In general, Article 28 prohibits the controller from using the services of processors who are unable or unwilling to provide enough guarantees to implement appropriate technical and organisational measures and operate in accordance with the security standards and data protection principles required by the Regulation. Data controllers who violate these clauses may be subject to significant administrative fines as well as legal action. The processor must put the necessary organisational and technological safeguards in place, must not hire sub-processors unless they adhere to the same degree of security, and must help the controller comply with the Regulation requirements.[37]

Further, the GDPR contains extensive rules on incident management and reporting to competent authorities, as well as to data subjects whose data were breached. The provisions in Section 2 of Chapter IV GDPR, which begin with measures ensuring the security of processing, notification of a personal data breach to the supervisory authority, notification of the breach to the data subject, and continue into Section 3 and the provisions regarding the data protection impact assessment, deal specifically with the controller's obligations with regard to information security. Article 32 of the Regulation establishes a requirement for data controllers to take into account the nature, scope, context, and purposes of processing, the likelihood and seriousness of risks to the rights and freedoms of data subjects that may result from the processing, as well as the cost of implementing the necessary technical and organisational safeguards.

Finally, a requirement under the General Data Protection Regulation (GDPR) calls certain organisations to appoint a Data Protection Officer (DPO). The DPO's duty is crucial for ensuring that personal data are protected within an organisation, reflecting and improving current information security standards and legal requirements.[38] Many industry standards, like ISO 27001 (Information Security Management), call for oversight of the security strategy by a person or group that must function independently of the organisational structure in order to prevent conflicts of interest. This is mirrored by the GDPR, which requires that the DPO work independently and not face repercussions for doing their job. Regarding specific expertise and knowledge, the GDPR requires that a DPO have a thorough understanding of data protection law and practices, much like how infosec standards call for staff to be adequately skilled and competent. Like their

[37] Ibid, Art. 28.
[38] Art. 37 GDPR.

counterparts in infosec roles, DPOs must have a thorough awareness of the organisation's technology, data processing activities, and risk landscape.

The identification, evaluation, and mitigation of risks are a key component of both the GDPR and information security laws and industrial standards. Organisations are required to undertake routine risk assessments and apply suitable steps to mitigate the risks highlighted by infosec standards like ISO 27001. Similarly, a DPO is in charge of determining the risks associated with data processing operations and ensuring GDPR compliance to reduce these risks.[39] The GDPR requires the data protection officer to help in educating and training staff members who are involved in data processing operations, consistent with information security standards' long-standing emphasis on staff education and awareness as a means of lowering the possibility of data breaches caused by human error. Finally, DPOs are tasked with overseeing an organisation's data protection initiatives and ensuring they comply with the GDPR, comparable to how information security standards call for recurring audits and assessments to guarantee continued adherence to the standards and applicable legislation.[40]

6. INFORMATION SECURITY RELATED PROVISIONS IN OTHER EU LEGISLATION

6.1. Digital Operational Resilience Act

The first draft of the Digital Operational Resilience Act (DORA),[41] which is a component of the Digital Finance Package (DFP), was released by the European Commission on 24 September 2020. This bundle includes a new retail payment strategy, legislative suggestions on cryptocurrency assets, blockchain technology, and digital operational resilience. It is common knowledge that the financial industry is becoming increasingly reliant on ICT and digital information. The COVID-19 incident also served as a motivator because financial institutions now rely increasingly more on the accessibility of digital technologies to carry out routine tasks remotely. The last few years have demonstrated how important digital resilience is, and how this dependence has drastically increased technology and cyber risk.

With DORA, the EU seeks to increase the financial sector's resistance to incidents involving ICT and imposes highly stringent, prescriptive rules that are uniform among all EU Member States. This new legislation also applies to crucial ICT third parties that offer financial institutions ICT-related services like cloud platforms, data analytics, and audit services. Organisations must be able to endure, respond to, and recover from the effects of ICT incidents in order to continue doing vital and crucial tasks while causing the least

[39] Arts 35 and 39 GDPR.
[40] Art. 37 and 39 GDPR.
[41] 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.

amount of interruption to consumers and the financial system. This is only possible by putting in place strong measures and controls on systems, tools, and outside parties, by having the appropriate operational continuity plans in place, and by continuously verifying their efficacy.

Organisations in the financial sector are required under DORA to implement and maintain resilient ICT tools and systems that lessen the impact of ICT risk. In order to implement protection and preventative measures, it is necessary to constantly identify all potential sources of ICT threats. It is important to detect out-of-order and potentially malicious activity quickly. Quick recovery from an ICT-related occurrence should be ensured by devoted and thorough business continuity policies and disaster and recovery plans. Processes should be created to adapt to external events as well as to the entity's own ICT mishaps.

The Regulation also lays out incident response responsibilities, requiring enterprises to set up and implement a management procedure to track and record incidents involving ICT. Under DORA, organisations are now required to determine the incident's classification using the standards outlined in the regulation, ensuring that incidents are reported to the appropriate authorities using a standard template and a standardised process as set forth by the relevant supervisory authority, and to provide users and clients of the company with first, interim, and final reports on ICT-related incidents (in a vein similar to GDPR incident reporting).

DORA introduces a requirement for organisations to conduct regular operational resilience evaluations, proportionate to the organisation’s size, business and risk profiles. Any vulnerabilities, defects, or gaps must be quickly found, corrected, or reduced by putting preventative measures in place.

Finally, the Regulation requires thorough monitoring of risks resulting from reliance on ICT third-party providers, providing mechanisms to enable organisations to harmonise critical aspects of service and relationships with ICT third-party providers to enable "complete" monitoring. Organisations are required to make sure that contracts with ICT third-party providers include all the information required for monitoring and accessibility, such as a detailed description of the level of service, a list of the locations where data are processed, etc.

6.2. Critical Entities Resilience Directive

In January 2023 the European Critical Infrastructure Directive adopted in 2008 was replaced by the Critical Entities Resilience Directive (CER).[42] The new Directive is designed to increase the vital infrastructure's resistance to a variety of dangers, such as

[42] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

terrorism, insider threats, natural disasters, and sabotage analogously to the NIS/NIS2 provisions concerning information security. Since the CER Directive covers more industries than its predecessor and places new requirements on firms that provide essential services, more businesses will be subject to the new regulations.

In contrast to the 2008 Directive, which covered only the energy and transportation industries, CER now covers nine more industries: banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space, and food. As a result, businesses involved in such industrial sectors have to determine whether the new regulations apply to them. Within nine months of notification, the critical entities must examine their operations, identify the pertinent risks, and take the necessary precautions to maintain resilience, updating the assessment every four years. All relevant natural and man-made hazards that could result in an incident, including those that are cross-sectoral or cross-border in nature, should be taken into account in the risk assessment. The critical entities will be required to put in place suitable and proportionate organisational, technical, and security measures to ensure their resilience in, among other things, preventing incidents, making sure that the premises are adequately protected physically, or responding to incidents and minimising their effects. Personnel training is also included in the measures. Finally, in the event of incidents or major interruptions, the critical entities have an obligation to alert the appropriate authority.

6.3. The Digital Services Act and the Digital Markets Act

The European Commission proposed the Digital Services Act (DSA)[43] in 2020, and it was formally adopted in November 2022. It is a key piece of legislation intended to modernise the legal framework for digital services in the European Union. The DSA is primarily concerned with issues relating to online content moderation, transparency, and the accountability of digital service providers. The Act does, however, include several provisions that indirectly relate to information security – the risk management obligations of very large online platforms, obligations related to the traceability of business users, and data access and transparency provisions. Very big online platforms are required by the DSA to manage systemic risks, particularly those affecting the security and integrity of their services. Although the DSA does not use the term precisely, information security hazards may theoretically be included in these dangers. In order to avoid, identify, or take action against suspected illicit content, the DSA requires online marketplaces to include the necessary safeguards to ensure the traceability of business users, which may also have an impact on information security, for instance by assisting in the prevention of fraud.

[43] 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.

Likewise, the Digital Markets Act was formally adopted in September 2022 with the goal of regulating giant tech firms, also referred to as gatekeepers, to ensure fair competition in the digital market.[44] While its main objective is to establish a free and open digital economy, some elements of the DMA might indirectly have a positive effect on the status of information security.

For example, the DMA mandates gatekeepers to provide real-time access to certain data and to ensure interoperability.[45] Although this provision is primarily an attempt to promote competition, it also has a tangential relationship to information security because gatekeepers have to grant such access in a secure manner to prevent vulnerabilities or a breach of user data by unauthorised third parties. Further, the DMA provides that data collected through the use of gatekeeper services has to be effectively portable.[46] While this increases user control over personal data, it also necessitates safe data transfer to ensure the confidentiality and integrity of the data, suggesting a concern for information security. Finally, gatekeepers are forbidden by the DMA to fuse personal data obtained from their services with other data unless the user has been given the option and has granted approval.[47] Indirectly, this provision follows GDPR data protection requirements and, with it, the immanent information security requirements.

6.4. The Data Governance Act

The Data Governance Act is a crucial component of a larger legislative initiative the EU has launched to establish regulations for future digitalisation, the data economy, artificial intelligence, and other critical policy objectives frequently referred to as digital sovereignty. Data are a key element in this paradigm, since artificial intelligence research depends on having access to vast data sets. Similar to this, the performance of almost all recent digital products, apps, and services for the information society depends in part on the availability of data. Finally, the accessibility of large amounts of data is becoming more and more crucial to scientific research as a whole.

The DGA has a wide range of goals. In an effort to catch up with the United States and Southeast Asia,[48] the birthplaces of the majority of today's innovative services and platforms, the main goals of the initiative are to improve the EU's digital single market and promote the European data economy. Small and medium-sized businesses (SMEs) and start-ups are given particular attention in an effort to support the entrepreneurial culture of the European market. These organisations profit particularly from intentional

[44] 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).
[45] Arts 2, 6 and 7 of the Digital Markets Act.
[46] Art. 6 of the Digital Markets Act.
[47] Art. 5.2 DMA
[48] W.G. Voss, "Cross-Border Data Flows, the GDPR, and Data Governance Cross-Border Data Flows, the GDPR, and Data Governance", Washington International Law Journal, Vol. 29, 2020.

data reuse and sharing, which offer fresh content for advancements in artificial intelligence and digital applications.[49]

The DGA seeks to create a unified market for data that will enable cross-sector data exchange inside the EU, allowing processing operations, news services and products for general public benefit. While data governance is the DGA's primary focus, several of its requirements are related to information security. The DGA creates a legal framework for companies which offer data sharing services. Such services are required to have the proper organisational and technical safeguards in place to guarantee that data are processed and shared securely. This includes defence against unintentional or accidental loss, change, disclosure, or access.[50]

The Act establishes the idea of personal data spaces, which are safe locations where people can view their data and decide who has access to it.[51] The provision emphasises the need for strong security controls to protect the personal data in these areas, even though it does not go into detail about specific security measures. To encourage data sharing while lowering privacy threats, the DGA emphasises anonymisation and pseudonymisation approaches.[52] These are data protection techniques, but they are also acknowledged as crucial information security measures. Data sharing service providers should have appropriate risk management mechanisms in place, and information security risks may fall under this category.

The Artificial Intelligence Act

The European Union's Artificial Intelligence Act,[53] which was introduced by the European Commission in April 2021 and approved by the European Parliament in 2023, intends to establish a thorough legislative framework for reliable and secure AI throughout the Union. The main goal of this proposal of a regulation is to establish a consistent legal framework that is in line with Union principles for the creation, promotion, and use of artificial intelligence. The Act would ensure the free cross-border movement of goods and services based on AI, preventing Member States from placing restrictions on the creation, marketing, and use of AI systems. It also pursues a number of overriding public interest objectives, including a high level of protection of health, safety, and fundamental rights.

Through a number of provisions, this proposal indirectly addresses information security by categorising AI systems according to their level of risk that their processing operations pose, demanding that a risk management strategy be in place throughout the whole

[49] J. Ruohonen, S. Mickelsson, "Reflections on the Data Governance Act", Digital Society, Vol. 2, 2023, https://doi.org/10.1007/s44206-023-00041-7.
[50] Chapter III of the DGA.
[51] Recital 30 of the DGA.
[52] Recital 32 of the DGA.
[53] 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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

lifecycle of high-risk AI systems.[54] The Act primarily focuses on the risk to fundamental rights and safety, and thus this requirement may also potentially include risks linked to information security.

The proposed law also places strong emphasis on the quality of the data used to develop, verify, and test high-risk AI systems.[55] It demands that the data be accurate, full, relevant, and representative. Although not stated directly, maintaining data quality is a key component of information security as it might result in inaccurate AI judgments that could have security repercussions.

To ensure results can be tracked, high-risk AI systems must keep activity records.[56] These records can be useful in locating and responding to security issues from the perspective of information security. AI systems must be created and developed in a way that guarantees their security, accuracy, and resilience over their entire existence. This includes resistance to both overt attacks and covert attempts to tamper with data or make predictions. Finally, high-risk AI systems need to be built to allow for human monitoring, which should be able to successfully reduce risks, including potential security issues. Human monitoring provisions are especially interesting from the comparative perspective, while they are underregulated in comparison to the GDPR DPO position or various information security adviser positions.[57]

6.5. Outstanding Regulation, Directive and Policy Proposals

Currently, the EU is working on several Regulation and Directive proposals ranging from the long outstanding ePrivacy Regulation Proposal to the relatively new Health Data Space Regulation, the European Chips Act and the Data Act Proposal. Several of the proposals being developed contain provisions related to information security.

The proposed *E-Privacy Regulation* is meant to replace the current E-Privacy Directive and increase privacy protection under the General Data Protection Regulation (GDPR). The requirements of the E-Privacy Regulation indirectly relate to information security since it compels service providers to safeguard the security of their services, even if its primary focus is on the secrecy of electronic communications and the restrictions for monitoring technologies such as cookies. The proposed Regulation requires confidentiality of electronic communications data and only allows their processing under specific conditions. The proposal also requires electronic communications service providers to implement appropriate technical and organisational safeguards to ensure the security of their services. The E-Privacy Regulation proposal, like the GDPR, includes provisions for notifying regulatory authorities and affected individuals in the event of an electronic communications data breach. Finally, the Regulation proposes strict rules on

[54] Title 3 of the Proposal of the Artificial Intelligence Act.
[55] Art. 9 of the AI Act.
[56] Ibid, Arts 11 and 12.
[57] Ibid, Art. 14.

unsolicited electronic communication (spam), as well as the use of cookies and other tracking technologies, and improving information security indirectly by limiting unnecessary data processing and collection.

The *European Health Data Space Proposal* aims to promote health-data exchange and research into new preventive strategies, treatments, medicines, medical devices, and outcomes. Given existing EU legislation, the EHDS proposal is expected to closely align with the General Data Protection Regulation (GDPR) and the Data Governance Act, which lay out guidelines for data protection, privacy, and secure data sharing. Provisions in the proposal ensure the safe and secure exchange of health data across the EU. To protect data during transit and storage, encryption, anonymisation, pseudonymisation measures and authentication mechanisms are proposed,[58] as well as provisions to protect individuals' health data, including strict controls over who can access the data and for what purposes. The proposal also mandates risk management systems for healthcare providers, researchers, and other relevant entities. These systems would be designed to detect and mitigate potential data security threats.[59] The proposal includes provisions for the timely reporting of security incidents, including data breaches, in accordance with GDPR requirements for data breach notification, as well as provisions for monitoring and enforcing compliance with the regulation's security requirements, including potential penalties for noncompliance.

The *European Cyber Resilience Act Proposal* is a proposal for an EU Regulation on horizontal cybersecurity requirements for products with digital elements.[60] Successful cyberattacks on hardware and software are becoming more common. Such products suffer from two major problems that increase costs for users and society: first, a general lack of cybersecurity, as evidenced by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them; and second, users frequently lack understanding and access to information, preventing them from selecting products with adequate cybersecurity properties or using them in a secure manner. In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, quickly spreading across internal market borders. This can severely disrupt economic and social activities and even endanger people's lives.

The *Data Act Proposal* seeks to prevent third-country unlawful transfer or access to non-personal data, supplementing the framework on international data flows established by the GDPR and the Data Governance Act. With growing concerns about industrial espionage, intellectual property (IP) theft, and unauthorised access to information by foreign authorities, the new rules prioritise the protection of commercially sensitive data

[58] Art. 23.3 of the EHDS Proposal.
[59] See also Chapter IX of the Regulation 2017/745 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
[60] Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454.

as trade secrets, as well as data subject to intellectual property rights or confidentiality obligations under European law. As a result, certain safeguards are put in place to ensure that the level of protection provided by the European regulatory framework is maintained when non-personal data are transferred outside the EU's borders.

To this end, data processing service providers must take all reasonable technical, legal, and organisational measures to prevent international transfers or governmental access to non-personal data held in the EU from conflicting with EU or national law (for example, commercially sensitive information, data that may affect security or defence interests).

Furthermore, third-country court judgments and administrative decisions requiring the transfer or access to non-personal data held in the EU will only be recognised or enforceable if they are based on an international agreement. Otherwise, such decisions must meet certain strict conditions for the transfer or for access to take place, and only the minimum amount of data permissible may be provided.

The *EU Cyber Diplomacy Toolbox* is a coordinated diplomatic response by the EU to malicious cyber activities.[61] This is part of the EU's approach to cyber diplomacy within the Common Foreign and Security Policy, and it contributes to conflict prevention, cybersecurity threat mitigation, and the greater stability of international relations. It has an impact on the behaviour of potential aggressors. The diplomatic response of the EU to malicious cyber activities is proportionate to their scope, scale, duration, intensity, complexity, sophistication, and impact. Through increased international cooperation, all diplomatic efforts promote security and stability in cyberspace and reduce the risk of misperception, escalation, and conflict that may result from ICT incidents.

Finally, additional proposals in the making, such as the *European Chips Act,* may contain provisions related to information security. As transition into the information society intensifies, considering information security requirements and building a resilient and efficient information security infrastructure are becoming an inescapable requirement when considering new legislation.

7. THE LEGAL FRAMEWORK OF INFORMATION SECURITY IN CROATIA

As the internet does not take into account national borders, the competences of the judiciary or other institutions of the state, it becomes imperative for cybersecurity laws to evolve in a manner that transcends traditional jurisdictional boundaries. This necessitates the establishment of international frameworks and cooperative agreements that enable effective enforcement and coordination among different national cybersecurity agencies. Problems in the availability and proper operation of internet services can have a significant negative impact on individual Member States or on the Union as a whole. The security of network and information systems is essential for the

[61] https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf.

smooth functioning of the internal market, but the security of systems that extend and operate on the territory of the entire Union and beyond cannot be achieved without broad consensus, cooperation and shared competences between the Member States.

The Croatian Information Security Act of 2007 represented the Croatian legislative interpretation of the requirements from the European Cybersecurity Strategy of 2001. The provisions of the Act apply exclusively to the work of Croatian public authorities, i.e. central, regional and local state administration, regulatory bodies and agencies.[62]

The Act, followed by a national implementing bylaw of a similar name,[63] defines information security concepts in Croatian legislation, also providing for information security measures and standards, areas of information security and security accreditation, regulates the application of relevant information security standards such as the ISO 27000 family of standards to the work and procedures of the state administration in the field of data classification, regulates the tasks and competences of information security advisers, and determines the categories of classified data and the conditions of their classification and use.

With respect to institutional development, the ISA regulated the establishment and status of the national CERT (Computer Emergency Response Team) assisting with processing and recording incidents of information security violations, i.e. criminal offences from Chapter XXV of the Criminal Code of the Republic of Croatia, including cooperation with the State Attorney's Office, the police and other bodies, as well as the State Information Security Bureau, a technical body tasked with developing and applying certification schemes and assisting with information security practices for the central, regional and local government and other public authorities.[64]

Reflecting on the almost twenty years of the application of the ISA, it is clear that its impact on the practice of maintaining information security within the framework of the activities of public authorities and other public institutions in Croatia was limited in scope from the start. The rising number of incidents, both of information security breaches as well as related personal data breaches, underscores the failure of the mostly normative only approach. Comparative legal experience shows that the adequate implementation of appropriate procedures and behaviour with the aim of preserving the confidentiality, availability and integrity of data is not the result of broad or even targeted legislative intervention, but of systematic education and the application of information security standards.[65]

With the NIS Directive, the European legislator at the highest level tried to establish cooperation groups composed of representatives of Member States, the Commission and

[62] Information Security Act (ISA), Official Gazette (OG) of the Republic of Croatia, OG 79/07.
[63] Art. 1 ISA.
[64] Arts 17-19 ISA.
[65] B. Bulgurcu, H. Cavusoglu, I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness", MIS Quarterly, Vol. 34(3), 2010.

ENISA. In order to support and promote strategic cooperation among the Member States regarding the security of network and information systems and for this group to be effective, it was necessary for all Member States to have a minimum capability and strategy to ensure a high level of security of network and information systems. The NIS introduced the obligation for Member States to appoint one or more computer security incident response teams (CSIRTs) – bodies or teams of experts to respond to security incidents. CSIRT or CERT (computer emergency response team) is a common name for groups of experts gathered to process and respond to security incidents related to the use of information systems and networks.[66] The CERT/CSIRT teams of the Member States are (now) responsible for monitoring security incidents at the national level, early warning and reporting information to relevant authorities about risks and incidents, responding to incidents, providing adequate dynamic analysis of risks and incidents and situational analysis, and participating in the network of national CSIRTs.[67]

In July 2018, as a transposition measure for the implementation of the NIS Directive into the Croatian legislation, the Croatian legislator passed the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers.[68] The Act regulates procedures and measures whose task is to achieve a high level of cyber security of key operators and providers of digital services. In addition, the competences and powers of competent bodies are regulated, a single national contact point is determined, and the competences and powers of bodies responsible for incident prevention and protection and other issues related to the institutional framework are also provided for by the provisions of the Act.[69] According to the provisions of the Act, providers of essential services are private law bodies (various commercial companies) and public authorities that play an important role in modern society and the economy. From the Croatian perspective, this is a particularly significant innovation in the context of the current regulation of information security, given that the current legal framework for information security is regulated by the provisions of the Data Confidentiality Act and the Information Security Act, which applied exclusively to public authorities.[70]

The central part of the Act refers to the identification of key service operators and digital service providers. In contrast to the existing regulations, primarily the Information Security Act, the provisions of the Cybersecurity Act refer to operators of key services and digital service providers who can be public or private entities in accordance with the criteria of the Act.[71] The Act regulates the identification procedure as well as the criteria for the effect of the incident on the availability of essential service, based on an assessment

[66] The name CERT historically belongs to the CERT Coordination Center of the US based Carnegie Mellon University, and as a generic name it came into wider use in the mid-1990s. The CSIRT variation arose in response to the need to differentiate CERTs from general technical support to emphasise the task of responding to security incidents.
[67] Art. 12 NIS Directive.
[68] OG 64/2018.
[69] Art. 1 ACOESDSP.
[70] OG 79/07, 86/12.
[71] Art. 5 ACOESDSP.

of the number and type of users to whom the service provider delivers the service, the existence of the dependence of other activities or areas on the provision of the service, the market share of the entity providing the service, the geographical spread of the entity in providing the service, the possible impact of the incident considering its severity and duration on economic and social activities and public safety, the importance of the entity's business for maintaining a sufficient level of key services, and other criteria such as the amount of service provided, the share in the provision of the service, or the entity's assets. [72]

The Act provides for the appointment of the Office of the National Security Council as a single national contact point. The tasks of the single national contact point were defined in Article 30 of the Act and include data exchange with the European Commission, participation in the work of the Cooperation Group established for the purpose of supporting and facilitating strategic cooperation and information exchange between Member States and developing trust and security at the EU level in terms of cyber security, forwarding at the request of the competent CSIRT notification of incidents to the unique contact points of other Member States, information on the number of identified operators of key services and notification of incidents, and of the development and harmonisation of the national cyber security strategy with the requirements of the Union, etc.[73]

Compared to the previous framework, the Act provides more detail on the question of the competence of CSIRTs and their obligations, which include monitoring incidents, providing early warnings and announcements, and informing about risks and incidents, conducting a dynamic analysis of risks and incidents and reviewing the situation in the sectors of their jurisdiction, conducting regular vulnerability checks of network and information systems of key service operators and digital service providers, receiving notification of incidents, at the request of key service operators and digital service providers, analysing and responding to incidents, informing the single national point about incidents and providing information on incident resolution procedures, making contact with the competent CSIRT body of another affected Member State, cooperating with other CSIRT bodies at national and international levels, participating in the network of CSIRTs at the EU level established with the aim of developing trust and confidence among Member States and promoting fast and effective operational cooperation.[74]

Another novelty in relation to the previous framework is a system of administrative fines for violations of the provisions of the ACOESDSP. Fines are provided for key operators and digital service providers who do not act according to the instructions of the competent sector body, who refuse to submit or unreasonably delay submitting notifications about incidents, if they fail to submit the data necessary to assess the level of security of network and information systems and evidence of the effective implementation of security measures, etc. Fines vary from HRK 15,000 to 50,000 for responsible persons in legal

[72] Ibid, Art. 7.
[73] Art. 30.
[74] Art. 32.

entities and public entities, from HRK 50,000 to HRK 150,000 for natural persons, craftsmen and other natural persons performing independent activities, up to the highest fines of HRK 150,000 to HRK 500,000 for legal entities and public entities. Interestingly, when adopting the Act, the legislator decided to keep the provisions on the liability of persons responsible in legal entities and public authorities.[75] Similar provisions were present in the old Act on the Protection of Personal Data, and which were curiously omitted in the process of passing the Act on the Implementation of the General Data Protection Regulation.[76]

8. CONCLUSION

The past fifteen years, especially the period from the adoption of the European Information Security Strategy to the adoption of the EU Directive on Information and Network Security, its subsequent transposition into the legal systems of the Member States of the EU, the adoption of the Cybersecurity Act and finally the adoption of NIS2, represent a relatively short period for the development of legislation, but at the same time it represents an extremely a long period for the development of information technology, services and the way we use information systems. As in the case of the development of the legal protection of personal data, the world has progressed rapidly compared to the previous period and presented new questions and challenges for legislators. New technologies such as widespread high-speed internet access (broadband), mobile networks with high data throughput, increasingly powerful mobile devices that surpass former desktop computers in terms of processing power, and sensors and data storage space make available to users a number of options and enable numerous new services that we collectively call services of the information society.

In the period that has passed since the adoption of the first proposals, we have witnessed the diversification of the profile of cybercrime perpetrators, the increased sophistication of attacks, the opening of new attack vectors and the commoditisation of malicious programs and services for attacks on information systems, which has been made possible by the development of DarkNet as a medium and cryptocurrencies as a means of anonymous payment. Recent developments in machine learning are also adding complexity to an already difficult situation. Numerous information services, especially social networks and location services, simultaneously represent a challenge both for the protection of personal data and for ensuring information security. Today, hackers can try to connect to one of the access points of a wireless local network from the lobby or the surroundings of a bank or some other institution or bypass the existing security infrastructure in some other way. Successful attacks compromise not only the service provider's information system, but also user accounts and potentially serve as a means of

[75] Arts 42 to 45 of the ACOESDSP.
[76] See Art. 36 of the Personal Data Protection Act (OG 103/03, 118/06, 41/08, 130/11, 106/12).

attacking other, related services. New forms of communication open up new opportunities for social engineering and identity theft.

In this landscape, the new European regulation in the field of information security is not only an attempt by the European legislator to introduce into national legislation legal concepts such as essential and digital services, but also a general effort to raise awareness of the importance of ensuring safe and secure use of information systems of importance for economic, administrative and general social life in the era of transition to the information society. So far, the fragmented market of digital content and services, and low productivity and innovation have turned, at least in the field of information technologies, the European Union into a second-rate power. The United States and Asian competitors, especially China, Japan and South Korea, are leading both in terms of research and development, as well as in terms of the commercialisation of these technologies. Although globalisation has affected all economic activities and branches, it is precisely the information technology market that is one of the most open and consequently most exposed to open global market competition. However, European inefficiency and stubborn insistence on narrow national interests against the consolidation of a common digital market over the past twenty years have resulted in the complete dominance of foreign, mostly American, products and services in the field of information technologies. Platforms like Google, Facebook, Uber, YouTube and many others are disrupting traditional business models in the fields of advertising, transportation, and the content industry. In economic terms, the European project needs a strong single internal market as a training ground for research, development and commercialisation of new products and services. In this sense, the NIS2 Directive and related legislative efforts in the regulation of information security represent a new step in fostering a safe and secure common digital market.

TRENUTNI I RAZVIJAJUĆI REGULATORNI OKVIR INFORMATIČKE SIGURNOSTI U EU I REPUBLICI HRVATSKOJ

Informacijska sigurnost bavi se osiguranjem pouzdanog, povjerljivog i pouzdanog rada informacijskih sustava te očuvanjem dostupnosti i pouzdanosti podataka, a njen okvir i sadržaj sve više se reguliraju zakonima. Istraživanja iz područja informacijske sigurnosti i kibernetičkog kriminaliteta pokazuju da je broj napada na informacijske sustave, kao i povreda osobnih podataka u porastu. Prakse informacijske sigurnosti više nisu samo stvar priznatih standarda industrijske samoregulacije, već su umjesto toga sve više u fokusu zakonodavaca u Europskoj uniji, kao i u komparativnom pravu. U posljednjih pet godina regulativa informacijske sigurnosti u Europskoj uniji doživjela je značajne promjene i proširenje kroz brojne uredbe, direktive i zakonske prijedloge koji su još uvijek u razvoju. Ovaj rad daje pregled i temeljnu analizu postojećeg pozitivnog pravnog okvira informacijske sigurnosti u Europskoj uniji i Republici Hrvatskoj sa sadržajnog i institucionalnog aspekta. Kronološki su navedeni pojedini propisi koji sadrže odredbe iz područja informacijske sigurnosti, a razmatraju se i de lege ferenda rješenja.

Ključne riječi: Informacijska sigurnost, NIS Direktiva, NIS2, Akt o kibernetičkoj sigurnosti, OUZP

Dr. sc. Tihomir Katulić, izvanredni profesor na Katedri za pravo informacijskih tehnologija i informatiku, Sveučilište u Zagrebu Pravni fakultet
Dr. sc. Hrvoje Lisičar, izvanredni profesor na Katedri za pravo informacijskih tehnologija i informatiku, Sveučilište u Zagrebu Pravni fakultet