Information Security in Principles and Provisions of the EU Data Protection Law

doc. dr. sc. Tihomir Katulić
Faculty of Law of the University of Zagreb,
Trg Republike Hrvatske 14, Zagreb, Croatia
E-mail: tihomir.katulic@pravo.hr

Dr.sc. Nikola Protrka
Police College Zagreb
nikola.protrka@vps.hr

ABSTRACT - Information security practices are a staple compliance mechanism ensuring the lawful processing and protection of personal data in the new European legal framework of Data Protection. Both the General Data Protection Regulation and the Regulation 2018/1725 on the protection of natural persons regarding the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data contain recognizable principles of and provisions regarding information security methods and practices. The purpose of this paper is to analyse the new EU data protection framework from the perspective of regulation of information security requirements, especially from the perspective of the data controllers and processors and their obligations to ensure conditions for lawful and secure processing of personal data and comply with potential data subject requests.

Key words: information security, GDPR, data protection, personal data

I. INTRODUCTION

Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, otherwise known as the General Data Protection Regulation is not just a fundemental stepping stone in development of the European personal data protection legislation and an instrument that enlivens the status of personal data protection as a fundamental right as recognized by the Article 8 of the Charter of Fundamental Rights of the European Union, it is also a groundbraking document in regulation of information security, probably equally important as the contemporary Network and Information Security Directive. [1]

As a Regulation directly applicable in Member State, it mandates a systematic application of best information security practices in a number of interesting ways, and in a moment defined by information security risks coming from ever widening array of sources and actors characterized by different motives, methodology and level of sophistication.

Yearly reports by relevant regulatory and governmental institutions in the field such as those done by the European Network and Information Security Agency (ENISA) and EUROPOL depict continuing rise in the number and complexity of detected attacks on information systems and data.[2]

Furthermore, established research describes an increase in massive, low-skilled attacks committed by perpetrators without advanced knowledge and understanding of information systems, often described as script-kiddies (*skiddies*).[3] Previously, in 2017, an EU Commission President Juncker repeated a finding that over 80% of European enterprises have suffered at least one case of information system attacks and that the volume of attacks has increased at rate almost 40% compared to the year before. [4]

Personal data has become a valuable commodity. Collection of massive amounts of personal data fuels modern information age economy. Through extensive and often sensitive profiling, data subjects and their personal data are objectified, often traded and exchanged even by the most scrupulous of actors in the data economy, let alone those who view personal data as raw industrial resource somehow disconnected from the lives and concerns of data subjects the data was harvested from.[5]

Since most of personal data collection, processing and storing is done through information systems an appropriate level of security of those systems is required to ensure the security of personal data. Some authors suggest recognizing data protection managament systems as a a paradigm of managing and ensuring security of processing of personal data. [6]

Where the data collected and processed is of sensitive nature, such as personal data containing or revealing racial or ethnic origin of data subjects, their political opinions, their religious or philosophical beliefs, trade union membership, or where data controllers process genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, the controllers are obligated to implement higher security measures and ensure a higher level of security to lessen the chance of a personal data breach.

This need to ensure a higher level of information security is not specific to handling special categories of personal data. In the information society economy and in the current threat environment, a higher level of information security is required to foster ongoing development of information society services. The European Commission and the lawmakers of Member States have repeatedly tried to regulate this requirement and improve the state of information security. Notwithstanding the Network and Information Security Directive and the national

transposition measures, the General Data Protection Regulation is the most recent example how information security principles and practices are making its way into law. Of course, one can argue that a normative approach alone will not be sufficient. However, an efficient and universally accepted legal and administrative regulation concerning information security is a requisite for transnational cooperation and a condition required to ensure that all actors participating in personal data processing and other information society services develop and enforce adequate security measures in order to prevent future personal data breaches.

The Regulation ultimately enforces these measures with potentially crippling fines, as well as establishing a framework for collective action against data controllers responsible for the breach of personal data, regardless of the source and perpetrators of the incident. This form of objective, strict liability only partially amenable through observing due dilligence on the behalf of the controller creates a significant burden, so there is a lot of incentive for data controllers to improve the security of processing.

The purpose of this paper is to discuss principles of information security and their application in the provisions of the General Data Protection Regulation and how they affect everyday practice of data protection and use of personal data.

II. INFORMATION SECURITY PRINCIPLES IN THE GENERAL DATA PROTECTION REGULATION

Even though the Regulation itself mentions the term „information security“ only once, it is nonetheless abundantly clear that recognized information security practices present a framework of ensuring accountability in personal data processing. [7]

In general, the provisions of the Regulation that concern information security strive to achieve several key objectives in order to facilitate data controllers accountability, a key principle of personal data processing that demands that the data processor be able to prove compliance with principles of personal data processing as stipulated by the General Data Protection Regulation.

In practice, as 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, unauthorized access to personal data, or other unathorized transmition, storage or processing of personal data – data controllers need to make sure they have proper security controls in place to be able to prove accountability.

This demands proper security controls with regard to access and identity management, ensuring that only employees that need access to personal data to conduct required processing operations actually have access, and that they have the lowest possible level of access that allows normal operation. Employees that handle personal data should receive adequate privacy training and additionaly adequate organisational measures such as non disclosure and confidentiality provisions need to be made part of employee contracts.

While not mandated by the Regulation, encryption and pseudonymization are specifically mentioned in the context of risk management and incident response, especially concerning the cases of obligation to notify data subjects that a breach has occured.

Data controllers also have an obligation to prepare for potential incidents and data breaches. Controllers have to be able to identify that a breach has taken place, do what needs to be done to contain it, recover personal data, resume operations and report the incident to supervisory bodies.

The Regulation defines the relations between data controllers and data processors in a more detailed fashion. The new provisions demand compliance from processors and subprocessors and give data controllers tools to ensure that their business partners are contractually obliged to comply with the Regulation's standards.

While many of these obligations existed in the previous legal framework, the Regulation was developed on the foundations of Article 29 Working Party opinions and guidelines and contains enforceable and concrete provisions.

Starting with the Article 5, the Regulation systematically introduces information security principles and practices as a compliance mechanism to ensure secure processing and protection of data subject rights. The Article states that personal data shall be processed in a manner that ensures appropriate security of the personal data. According to Article 5, this manner of processing includes both protection against unauthorised or unlawful processing of personal data as well as additionally protecting against accidental loss, destruction or damage. Data controllers, data processors and others are required to achieve this using appropriate technical or organisational measures, a principle of *integrity and confidentiality* – well known components of the so called CIA triad of information security – confidentiality, integrity and availability. [8]

III. INFORMATION SECURITY AND DATA CONTROLLER OBLIGATIONS

In Chapter IV of the Regulation, Article 24 lays out responsibilities of the data controller. The data controller can be any legal person or natural person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. [9]

The article states that controllers shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed safely and securely in accordance with the Regulation. The controllers are required to take into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons whose data is being processed. Article 24 mandates implementation of appropriate data protection policies and regular review and update of technical and organisational measures where necessary. These provisions are accompanied by several recitals that establish the liability of the data controller for the safety and security of processing conducted by him or on his behalf, an obligation to implement appropriate and effective measures and ability to demonstrate that he is performing processing in compliance with the Regulation.[10]

Recital 75 of the Regulation states that risk to the rights and freedoms of natural persons coming from personal data processing may potentially lead to various consequences such as physical, material or non-material damage,

discrimination, identity theft, fraud, financial loss, damage to reputation, breach of professional secrecy etc. The recital also explicitely mentions situations where data subjects might be unable to exercise their rights and freedoms, control their data or when data processed might reveal sensitive data.

Additional situations mentioned by Recital 75 where processing activities pose recognized risk to the rights and freedoms of natural persons are those that concern analysing individual's performance at work, his economic situation, health, personal preferences or interests, location or movements of individuals in order to create or use personal profiles. It also underlines situations where data processed is the personal data of vulnerable natural persons, in particular of children, are processed or where processing involves a large amount of personal data and affects a large number of data subjects as those that pose risk.

The following Recital 76 refers to the obligation of the data controller to determine and assess the likelyhood and severity of the risk to the rights and freedoms of data subjects by taking into consideration criteria such as nature, scope, context and purposes of the processing.

Finally, Article 25 stipulates the obligation of the data controller to implement technical and organisation measures such as pseudonymisation, designed to implement data protection principles such as data minimisation and integrate them into its processing operations. When data controllers develop new applications, services and products based on processing of personal data, the controllers should develop them with data processing principles in mind from the start. The controller should also process only personal data necessary for specific purpose of processing, with regard to the amount of data, extent of processing, period of their storage and accessibility, ensuring what the Regulation calls data protection by design and by default.

IV. DATA PROCESSOR OBLIGATIONS

Another key issue the Regulation addresses is the relationship between data controllers and processors. This relationship in the past was subject to criticism concerning the ability of the controller to realistically enforce data protection measures and obligations on organisations doing the processing work on his behalf.

This is why Regulation Article 28 now explicitely regulates the relationship between data controllers and data processors. Data processor can be a natural or legal person, a public authority, an agency or any other body which processes personal data on behalf of the controller.

The processor receives personal data provided by the data controller and acts according to specific instructions issued by the controller. Generally, the Article 28 forbids the controller to use the services of processors who are unable or unwilling to supply sufficient guarantees to implement appropriate technical and organisational measures and function according to the security standards and data protection principles demanded by the Regulation. Failure to comply to these provisions could put data controllers at risk of large administrative fines as well as civil lawsuits.

At the same time, Article 28 regulates the obligation for data controllers to contractually or otherwise stipulate that processor acts only on documented instructions only, employs persons under adequate confidentiality regime by means of a contract or statutory obligation etc. The processor is required to implement all appropriate technical and organisational measures, can not engage subprocessors without ensuring their adherence to same level of security, assists the controller in complying with provisions of the Regulation and at the choice of the controller is obliged to return or delete all personal data belonging to the data controller.

V. INCIDENT MANAGEMENT AND REPORTING

Section 2 of the Chapter IV of the GDPR contains a number of provisions dealing directly with obligations of the controller with respect to information security, starting with the measures ensuring security of processing, notification of personal data breach to supervisory authority, communication of the personal data breach to the data subject and continuing into Section 3 and provisions regarding data protection impact assessment.

The Article 32 of the Regulation introduces an obligation for the data controllers to consider the nature, scope, context and purposes of processing, the likelihood and severity of risks the processing may pose to the rights and freedoms of data subjects and with all that in mind consider the state of the art and the costs of the appropriate technical and organisational measures.

The Regulation follows to specifically name pseudonimysation, encryption, efforts to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, ability to restore systems and data to a state of availability etc. Finally, the Regulation expects that data controllers will implement adequate processes to regularly test, assess and evaluate effectiveness of technical and organisational measures meant to ensure the security of processing.

It is apparent that the Regulation now introduces a requirement for data controllers to notify national supervisory bodies should a personal data breach occur – a similar requirement that has for some time existed in the legislation regulating electronic communications and financial services both in EU legislation and in national legislation.[11]

While some of the data protection authorities have previously encouraged controllers to report breaches, the 1995 Data Protection Directive 95/46/EC which was mostly transposed into national legal systems of Member States by 1998 and adopted by all new Member States in the following decades did not contain such requirement. The General Data Protection Regulation in Article 34 now mandates controllers to notify the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of individuals, and also to communicate a breach to the individual if it is likely to result in a high risk to their rights and freedoms. This puts forth certain obligations to controllers, namely to choose and apply adequate technical and organisational measures in relation to a required level of security of processing, which in turn is proportionate to the potential risks to rights and freedoms of data subjects whose data is being processed. The question of qualification of high risk

The controllers need these technical and organisational measures to detect potential breaches and prevent them, to discover ongoing security incidents to be able to report them and act in the interest of data subjects and to resume normal operation as soon as possible. The broad obligations set in

Articles 32 and 33 of the Regulation have been investigated and commented upon in the Article 29 Data Protection Working Party Guidelines on Personal Data Breach Notification under Regulation 2016/679 (GDPR) whose latest revised and adopted document was made available in early 2018. [12]

The central issue in complying with the provisions of Article 33 of the GDPR is the definition and meaning of the term data breach itself. Guidelines establish that a data breach is a type of security incident where a breach of personal data occurs and leads to any of a number of events and results such as accidental or unlawful - destruction of personal data, loss of personal data, alteration, disclosure, access to personal data, transmission, storage or some other accidental or unlawful kind of processing.

A previous WP29 Opinion 03/2014 provides a categorization of personal data breaches following well known security principles of confidentiality, availability and integrity. An integrity breach would involve alteration of personal data, confidentiality breach an unauthorized disclosure or access to personal data and an availability breach would correspond to accidental or unlawful destruction or loss of personal data.[13]

A matter raised in the Guidelines concerns criteria to establish wether a an availability breach has taken place. They offer examples of a loss of availability where an intentional deletion or deletion by accident occurs, where in the case of use of encrypted data a decryption key has been lost or where ability to restore data from backup is lost and is not possible to restore access to backedup data. Another given example of a loss of availability is when a significant disruption to the normal service occurs due to factors such as cyber attacks (i.e., denial of service attacks, malware attacks etc.) or infrastructure events such as power failure.

Regarding the obligation of data controllers to report temporary loss of availability as a data breach, Regulation Article 32, Guidelines explain that controllers should assess the likelihood and severity of impact on the rights and freedoms of natural persons as a result of the disruption in availability of their data and notify the supervisory authority unless the temporary breach is of such nature that it is unlikely to result in a risk to individuals' rights and freedoms.

With that in mind, the Regulation in Article 33 lays down the obligation of data controllers to notify the supervisory authority that a personal data breach has taken place. The Article regulates that the controller has an obligation to notify the authority no later than 72 hours after becoming aware of the personal data breach unless the data breach is unlikely to result in a risk to rights and freedoms of natural persons. Data processors are mandated to notify their data controllers immediately without delay after becoming aware of the data breach.

The Article 33 goes on to describe what a notification of personal breach to supervisory authority will consist of, mandating that data controllers:

- Describe the nature of the personal data breach including categories and number of data subjects potentially affected and personal data records concerned;
- Communicate the name and contact details of the data protection officer or other contact poitn where mroe information can be obtained
- Describe the likely consequences of the personal data breach etc.

The Article also stipulates that data controllers have to document any personal data breaches and relevant data, effects of the breach and whatever action they have undertaken to remedy and resume normal operation in order to verify compliance with the Regulation.

VI. NOTIFICATION OF DATA SUBJECTS

The provisions of the paragraph 1 and 2 of the Article represent an important compliance mechanism. Complying with these provisions basically demands that data controllers implement an information security policy, possibly invest in some sort of information security management system and educate their employees on the fundemental tenets of information security.

In that regard, information security standards such as ISO 27000 family of standards contain useful controls that cover relations with suppliers, issues of physical security, use of cryptography, management of assets, implementation of information security policies and human resources as well as handling incident response obligations.

Especially sensitive is the requirement regulated by the Article 34 that regulates the obligation to communicate that a data breach has taken place to the data subject. Should a personal data breach be likely to result in a high risk to the rights and freedoms of natural persons, the controller has to communicate the personal data breach to the data subject without undue delay. The contents of this communication mirror the provisions of Article 33, with addition of being described in clear and plain language understandable to the data subject. Guidelines offer criteria to distinguish risk and high risk, and assessment should take into account factors such as the type of the data breach, nature, sensitivity and volume of personal data, ease of identification of individuals, severity of potential consequences, special characteristics of the individual and the data controller, number of affected individuals etc. On the basis of the Personal Data Breach Severity Assessment Methodology developed by the European Network Information Security Agency, a free personal data breach notification tool was developed to help controllers report personal data breaches to competent authorities and assess the severity of the breach. [14]

However, should conditions exist such as use of appropriate technical and organisational measures that render personal data unintelligible to non-authorized users, or measures undertaken that prevent high risks to freedoms and rights of data subjects from materializing, data controllers would not be in obligation to notify data subjects. This provision creates an incentive for data controllers to implement these measures into their systems in order to lessen their potential liability.

These obligations form Article 34 will likely result in several outcomes. What has already happened is that the number of complaints, especially against Big Data companies and leading Internet platforms is on the rise, resulting in increased regulatory oversight and legal proceedings. According to the European Commission data, over 95 thousand complaints have been introduced between 25th of May 2018 and 28 of January 2019. [15]

The other outcome is favourable to information security industry, which is recording growth, development of new

tools and services aimed at connecting existing information security resources, standards and services for use in assuring data protection compliance.

With new provisions regarding collective legal actions in mind, it is obvious there is an increasing likelyhood of potentially crippling lawsuits to go along with already very strict administrative fines, justifying the spur in spending and investment into data protection compliance not just from major internet platforms and Big Data market players.

VII. DEVELOPMENT, COMPETENCE AND ROLE OF DATA PROTECTION OFFICERS

Data Protection Officer as an institute of data protection law first appeared in the West German *Bundesdatenschutzgesetz* in 1977, and subsequently in data protection regulation of several other European countries even before the adoption of Data Protection Directive in 1995. Not many countries however opted to regulate the data protection officer position and function. [16]. In Regulation 45/2001 designation of the DPO became mandatory for EU bodies and institutions.

There were and are various reasons for implementing a DPO as an institute of data protection law. Data protection legal framework is becoming increasingly complex in light of the technological an sociological changes due to the ongoing information revolution. To comply with these provisions, data controllers need specialized knowledge and skills. Secondly, the development of the applicable legal framework is demanding. National supervisory bodies, European data protection board (formerly the Article 29 Working Party) publish an increasing number of opinions and guidelines that direct and form the practice of data protection in the EU. Thirdly, the common digital single market represents a challenge with respect to handling data subject requests possibly coming from different Member States and cooperating with their national supervisory bodies. All these tasks expect a level of expertise many controllers simply cannot have within the ranks of their employees.

These reasons have contributed to the expanded and more elaborate regulation regarding data protection officers in the GDPR. Section 4 of the Chapter IV of the GDPR regulates the obligation to designate data protection officers, their position and their tasks in Articles 37 to 39.

In contrast to older practice of quantitative criteria for the obligation to designate data protection officers, such as when data controller employs twenty or more employees as was regulated in the former Croatian Personal Data Protection Act, the Regulation adopts qualitative criteria taking into account the status of the data controller, the purpose and scope of processing and wether large scale of special categories of personal data and personal data relating to criminal convictions are being processed.[17]. The Regulation explicitely provides for the possibility of having an outsourced data protection officer on the basis of a service agreement.[18]

The Regulation also elaborates on the expected competences and expertise of the data protection officer, stipulating that the data protection officer will be designated on the basis of professional qualities and expert knowledge of data protection law and practices, and the ability to fulfil the tasks of the data protection officer regulated in the Article 39: inform and advise the controller or processor and the employees on their obligations, monitor compliance with the Regulation, cooperate with the data protection supervisory authority and act as a contact point on issues relating to processing etc.

There are many parallels between data protection officers and information security advisers and chief information security officers that have sporadically been regulated in national legal system of Member States [19]. Regarding information security policies, both categories of experts have a role developing and managing the policies, even if the information security experts take on a more technical role and manage the tehnical implementation. Where DPOs help develop privacy policies and website notices, policies on use of social media, employee policies and codes of conduct, the information security advisers monitor implementation and adherence to security standards and requirements, access control and monitoring etc.

Both of these functions participate in managing the relations with service and product vendors, especially concerning their safeguards, security policies and procedures, previous incidents and data breaches and potential sharing of sensitive information. Normally, when present in an organisation, they usually coordinate management and response to data breaches and coordinate employee training.

VIII. DATA PROTECTION IN EU INSTITUTIONS

A few years after the adoption of the Data Protection Directive and following its transposition into national legal systems of Member States, EU adopted an acompanying Regulation (EC) No 45/2001 that provides natural persons with legally enforceable rights, specifies the data processing obligations of controllers within the Community institutions and bodies, and creates an independent supervisory authority, the European Data Protection Supervisor.

The EDPS is a supervisory body intended to oversee data protection in EU institutions and is responsible for monitoring the processing of personal data by the Union institutions and bodies. The EDPS monitors activities that use personal data of anyone who works with the EU, contractors and beneficiaries of various grants, even the visitors of EU institutions and bodies, and also consults DPOs of EU institutions, gives out advice in opinions, comments and decisions, raises awareness, conducts data protection audits to verify compliance etc.

Since the GDPR introduced new, more elaborate data protection rules for the dana controllers in the EU, it was necessary to develop the legal framework applicable to EU institutions that would provide EU citizens with the same level of security and assurance that they can enjoy when dealing with other data controllers under the General Data Protection Regulation. The EU law makers recognized importance of a coordinated and equivalent approach to personal data protection to align as far as possible the data protection rules for Union institutions, bodies, offices and agencies with the data protection rules adopted for the public sector in the Member States. This is why a second Regulation, the Regulation 2018/1725 concerning protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and

repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC was enacted in 2018.

These two Regulations follow the same principles, and they should be, from the perspective of judicature of the Court of Justice of the EU be treated as a common and equivalent legal framework.

Concerning relevant information security provisions, Article 4 of the Regulation 2018/1725 mirrors the Article 5 of the GDPR, maintaining that one of the general principles of processing of personal data shall be to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Regulation continues to copy provisions of the GDPR concerning obligations of data controllers (Article 24 of the GDPR into Article 26), data protection by design and by default (Article 25 of the GDPR into Article 27), regulating the relations between the data controller and the processor (Article 28 of the GDPR into Article 29), maintaining records of processing activities (Article 30 of the GDPR into Article 31).

Likewise, provisions of the Article 32 of the GDPR on security of processing are mirrored in Article 33 of the Regulation 2018/1725 with a minor difference in paragraphs 3 and 4, which have switched place so that Article 33 of the Regulation 2018/1725 puts the obligation of the controller and the processor to take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless required to do so by Union law, before the provision concerning adherence to an approved code of conduct.

The newer Regulation does however include a new section 3 in the Chapter IV. The new section is labeled *Confidentiality of electronic communications* and consists of three new articles regulating confidentiality of communication, protection of information processed by users' terminal equipment and contained in the directories of users.

Article 36 regulates that Union institutions and bodies shall ensure the confidentiality of electronic communications, in particular by securing their electronic communications networks.

Article 37 relates to protection of information transmitted to, stored in, processed and collected from users' terminal equipment and regulates that Union institutions and bodies have an obligation to protect such information collected from users accessing publicly available websites and mobile applications. Recital 54 of the Regulation further explains this point in reference that Union institutions and bodies, with respect to Article 7 of the Charter of Fundamental Rights of the European Union should protect such communications and related informationas Article 7 regulates that everyone has the right to respect for private and family life, home and communications.

Finally, Article 38 concerns the directories of users maintained by the institutions and bodies of the EU, and regulates that access to personal data contained in these directories and directories themselves has to be limited to what is strictly necessary for the specific function of the directory.

Section VI of the Chapter IV in Articles 43 to 46 contains adapted regulations concerning the status, position and tasks of data protection officers in the institutions and bodies of the EU.

There are several key differences between the GDPR and the Regulation 2018/1725 in this regard. For one, the newer Regulation reduces the possibility of an externalized data protection officer acting on the basis of a service agreement, which was one of the more interesting features of the Article 37 of the GDPR.

While still possible, the use of externalized DPO is now secondary choice. Paragraph 4 of the Article 43 states that the data protection officer shall be a staff member of the Union institution or body, and that Union institutions and bodies *may* designate a data protection officer on the basis of a service contract only when taking into account their size and if their organisational structure and size prevents them from designating a data protection officer, presumably because conditions of designating a person with adequate professional qualities, expert knowledge of data protection law and practices and the ability to fulfil DPO tasks are not met.

IX. CONCLUSION

In twenty four years since the EU adopted the Data Protection Directive in 1995, there has been a substantial amount of regulatory and practical progress both in the field of personal data protection and in regulation of information security. Especially in the recent years, in the judicature of national courts, the EU Court of Justice[20] and in the proceedings involving national supervisory bodies the rising number of cases have affirmed the status of personal data protection as a fundamental right.[21]

Information revolution and development of information society on the back of rapid technological development have sped up the adoption of relevant regulation much beyond the usual speed of legislative development. This in turn has created a substantial pressure on data controllers to invest in compliance in a field that was almost ignored just a decade ago.

Regulatory and practical issues of personal data compliance and information security compliance are, from the perspective of current European legal framework, intrinsically connected. The personal data protection framework has obviously, from the fundamental principles of processing such as the integrity and confidentiality principle through regulation of technical and organisational protection measures, incident reporting responsibilities and the designation and tasks of data protection officers adopted practices similar to those that have evolved in information security practice in roughly the same time period. This is a natural consequence of the fact that personal data is data processed and stored mostly in information systems, and security of information systems is vital for security of personal data. It also underlines a need for further research and development of safer information systems, applications and practices.

The efforts of the EU lawmakers, within the wider initiative to create the unified legal framework for the European digital single market have largely succeeded in the field of data protection. For different reasons, notably the fact that Member States' legal systems often consider information security an aspect of national security, the development of the common European legal framework in the field of information security has not been as succesful.

Hopefully, some of those solutions will eventually be applied to future EU common regulation of information security.

REFERENCES

[1] 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

[2] ENISA Threat Landscape Report 2018, European Network and Information Security Agency, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[3] Dragičević, D. i suradnici.: Pravna informatika i pravo informacijskih tehnologija, Narodne Novine, Zagreb, 2015.

[4] European Commission: State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber attacks, available at: http://europa.eu/rapid/press-release_IP-17-3193_en.htm

[5] Schwarz, P.M.: Property, Privacy and Personal Data, 117 Harv. L. Rev. 2056 (2003-2004)

[6] Voigt, P., von dem Busche, A.: The EU General Data Protection Regulation: A Practical Guide, Springer, 2017.

[7] Recital 49 of the 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, GDPR) (Text with EEA relevance), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[8] Andress, J.: Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Syngress, Elsevier, 2011.

[9] Article 4 and 8 of the GDPR.

[10] Recital 75 and 76 of the GDPR.

[11] I.e., Regulation 611/2013of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

[12] Article 29 Data Protection Working Party: Guidelines on Personal data breach notification under Regulation 2016/679, October 2017, rev. February 2018.

[13] Article 29 Data Protection Working Party: Opinion 03/2014 on Personal Data Breach Notification, March 2014.

[14] Personal data breach notification tool, ENISA, available at: https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

[15] GDPR in Numbers, GDPR Today, no.2, 28 Jan 2019, available at: https://www.gdprtoday.org/gdpr-in-numbers-3/

[16] Article 29 Data Protection Working Party: Guidelines on Data Protection Officers, December 2016, rev. April 2017.

[17] Article 18 Croatian Data Protection Act - Zakon o zaštiti osobnih podataka, Official Gazzette/ Narodne Novine 103/03, 118/06, 41/08, 130/11, 106/12, 26.9.2012.

[18] Article 37 of the GDPR.

[19] Information Security Act – Zakon o informacijskoj sigurnosti Official Gazzette/Narodne Novine 79/07, 30.7.2007.

[20] European Court of Justices cases C-131/12, Google Spain Sl. v. AEPD & Mario Costeja Gonzalez; C-362/14, Schrems v. Data Protection Commissioner; C-073/16, Puškár v. Finančné riaditeľstvo Slovenskej republiky; C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH; C-136/17, G.C., A.F., B.H., E.D. v Commission nationale de l'informatique et des libertés (CNIL); C-040/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V., joined parties Facebook Ireland Limited, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

[21] Article 4 of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.