The common EU approach to personal data and cybersecurity regulation

International Journal of Law and Information Technology, 2020, 28, 297–328
doi: 10.1093/ijlit/eaaa021
Advance Access Publication Date: 25 January 2021
Article

OXFORD

The common EU approach to personal data and cybersecurity regulation

Alessandro Mantelero*, Giuseppe Vaciago†, Maria Samantha Esposito* and Nicole Monte*

ABSTRACT

Several sector-specific studies on EU data protection and cybersecurity frameworks can be found in the literature, but their differing legal domains has hindered the development of a common analysis of the different sets of provisions from a business perspective. This article sets out to bridge this gap, providing a systematic review and a cross-cutting operational analysis of the main legal instruments that constitute the common European approach to personal data and cybersecurity regulation for the business sector. We aim to demonstrate the existence of a core of common principles and procedural approaches referring to specific cybersecurity and data security technologies. Analysis reveals a coordinated regulatory model based on five pillars: risk-based approach, by-design approach, reporting obligations, resilience and certification schemes. We also highlight the relationship between the main directives and regulations.

KEYWORDS: cybersecurity, data protection, eIDAS Regulation, NIS Directive, PSD2 Directive

INTRODUCTION

There are several sector-specific analyses of EU data protection and cybersecurity directives and regulations, but the different legal domains—private or administrative law for data protection, criminal law for cybersecurity—has prevented the

* Politecnico di Torino, C.so Duca degli Abruzzi 24, Torino, Torino, Italy. E-mail: alessandro.mantelero@polito.it

† Università dell'Insubria, Via Ravasi 2, 21100 Varese, Italy. This study was coordinated by A.M., who was the author of 'Introduction' and 'Coordinated analysis of the legal instruments examined' sections (with G.V.) and 'Conclusion' section; M.S.E. is the author of section 'Regulation (EU) 2016/679'; Sections 'The Payment Services Directive framework and security obligations', 'The Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)' and 'The NIS Directive framework and security obligations' were co-authored by N.M. and G.V. This research was partially funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 830929 (Cybersecurity for Europe project). The authors would like to acknowledge the helpful feedback received from the reviewers at *International Journal of Law and Information Technology* in preparing this article for publication.

development of a joint analysis of these different sets of provisions from a business perspective.[1]

This artificial distinction between these realms—data protection and cybersecurity—has two detrimental effects. First, the legal debate considers as separate a number of obligations and procedures that are often deeply interrelated in the daily business activities of many companies. Secondly, sector-specific analysis fails to reveal the common approach of EU regulation and therefore acts as an obstacle to the development of an integrated model for legal compliance and the avoidance of sanctions.

Moreover, data-intensive technologies and datafication of social environment require effective and integrated implementation of existing provisions with a focus on procedural and technological requirements, not limited to the theoretical foundations of data protection and cybersecurity.[2]

This article aims to bridge these gaps by providing a coordinated analysis of the legal instruments that have the greatest impact on the day-to-day processing operations of private companies. Without the ambition to cover all the existing regulations in the fields examined (eg criminal proceedings collaboration), four key regulatory instruments for business in the field of data protection and cybersecurity are considered: the General Data Protection Regulation (GDPR), the NIS Directive, the PSD2 Directive and the eIDAS Regulation.

While the GDPR provides the general framework for business activities based on personal data, the NIS Directive increases the level of resilience of critical infrastructure against cybersecurity risks, the PSD2 Directive promotes the development of advanced payment instruments and increases the security of the system, and the eIDAS Regulation supports the integration of digital identity and trust services into application services. In a nutshell, the GDPR has a more general vision, while the other regulations have a more specific vision (ie critical infrastructure, advanced payment and digital signature), but all four regulations have common features with regard to technical and organizational measures to protect data.

We do not include the Cybersecurity Act[3] in this analysis, since the relevant section of this regulation (Title III on the cybersecurity certification framework) provides only general guidelines which have yet to be implemented in concrete certification schemes.

By carrying out a cross-cutting operational analysis, these legal instruments are not considered in their main objectives and foundational principles, but in their operational and technological implementation. This makes it possible to go beyond a fragmented picture of different legal instruments, due to the sectoral approach of the

1 See also D Markopoulou, V Papakonstantinou, P de Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation' (2019) 35(6) *Computer Law & Security Review* 1–11. https://doi.org/10.1016/j.clsr.2019.06.007.

2 See in this respect the concrete and proactive approach adopted by EU bodies such as the EDPS, with the IPEN network and the ENISA. See EDPS, IPEN - Internet Privacy Engineering Network, <https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en> accessed 31 July 2020; ENISA, On-line tool for the security of personal data processing <https://www.enisa.europa.eu/risk-level-tool/> accessed 31 July 2020.

3 Regulation (EU) 2019/881 on ENISA (European Union Agency for Cybersecurity, formerly the European Network and Information Security Agency) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

EU legislator, and to reveal common regulatory patterns that facilitate companies to cope with the whole regulatory framework in a more systematic way.

As regards the level of detail of this analysis, at this stage of the implementation of the legal instruments examined, it is not possible to provide a fully integrated picture of the various obligations making up the common regulatory framework as the GDPR is mainly a principles-based regulation and two of the other three instruments are directives. However, we were able to achieve two key objectives: (i) identify the common patterns of obligations deriving from the various instruments; (ii) highlight the relations between these obligations, including the technology-based organizational and security measures.

This not only represents a basis for a future integrated compliance model, but also a steppingstone for rule makers towards a more comprehensive technical and legal harmonization of the different obligations in the national implementation of the framework in EU member states.

From this perspective, following this introduction, we examine the general framework provided by the GDPR, which sets out the overall principles for data processing, before going on to look at the various sector-specific regulations (PSD2 Directive, eIDAS Regulation and NIS Directive), which apply these regulatory principles in detail. Each legal instrument is briefly introduced, followed by an analysis of the relevant cybersecurity obligations and a table showing the relationships between the legal provisions and the associated technological and organizational measures. This makes it possible to identify the key operational and technical elements of the European approach at sectoral level.

As the aim of this article is to reveal the relationship between the obligations and requirements laid down by these legal instruments, the last two sections move from the sectoral level to the systematic level, identifying the common core of these instruments, both in terms of common principles and procedural approaches, and the specific cybersecurity and data security technologies. A coordinated harmonious model is revealed, based on five pillars: risk-based approach, by-design approach, reporting obligations, resilience and certification schemes.

REGULATION (EU) 2016/679

Although the GDPR focuses on the protection of personal data and data subject's rights, in line with the European tradition,[4] the means to achieve its goal are deeply rooted in the technological and organizational measures necessary to create a safe environment. The main objective of the legislator is to prevent potential risks and prejudices rather than imposing sanctions for violations.

From the outset,[5] data protection law has therefore been focused on risk, though over the years this risk has evolved in a variety of ways.[6] Moreover, from a regulatory

4 See G González Fuster, *Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014).

5 See AF Westin, *Privacy and Freedom* (Atheneum 1970).

6 See A Mantelero, 'Comment to Articles 35 and 36', in M Cole, F Boehm (eds) *GDPR Commentary* (Edward Elgar Publishing 2020, forthcoming) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3362747> accessed 21 February 2020; V Mayer-Schönberger, 'Generational Development of Data Protection in Europe?', in PE Agre and M Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997), 221–25.

perspective, data protection laws have also been characterized by a procedural approach.

These two elements are closely intertwined, as the focus on data management procedures, including data protection technologies, represents a form of risk management based on the regulation of the different stages of data processing, the definition of the powers and duties of the various subjects involved in the process, and the adoption of appropriate security measures.

Against this background, Regulation 2016/679 (GDPR) does not constitute a substantial paradigm shift,[7] although it does introduce new and specific provisions which emphasizes the role of accountability, risk management[8] and data security.[9]

In this context, the security obligations are designed not only to prevent data breaches and cyberattacks, but also to achieve the broader goal of ensuring the functioning of ICT systems, their interoperability and, more in general, their reliability. Ensuring data security is therefore not an isolated obligation grounded only on a few specific provisions in the GDPR but should be considered in the broader perspective of the accountability framework which data controllers must put into practice in accordance with the Regulation.

Controllers[10] are required to take both organizational and technical steps to ensure an appropriate level of personal data security and, therefore, the protection of the data subject's fundamental rights and freedoms. The GDPR stresses the need to consider privacy and data protection at the design phase and throughout the entire data lifecycle, as well as the need to put into place appropriate technical and organizational security measures to implement privacy and data protection principles.

GDPR and security obligations

In order to ensure the protection of personal data, data controllers and processors have specific security obligations, covering both technical and organizational measures, which directly or indirectly increase the level of IT security.[11] These obligations

7 See eg Directive 95/46/EC, arts 17 and 20. The Regulation is intended to strengthen the harmonization process that began with the 1995 Directive, and the new provisions necessarily remain on the same path.

8 In accordance with traditional risk analysis models, the GDPR prescribes a multi-stage process for impact assessment and risk management, based on the following five phases: an analysis of the envisaged processing, an assessment of the risks to the individual's rights and freedoms, the identification of the measures to address these risks, the verification of the effectiveness of these measures and their periodic updating. See Article 29 Data Protection Working Party. '*Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*'. Adopted on 4 April 2017, as last revised and adopted on 4 October 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (3 February 2020, date last accessed).

9 The GDPR adopts a risk-based approach not only in defining specific data security obligations but requiring a risk management strategy, as demonstrated by the controller's obligations concerning the records of the processing activities (art 30), data protection impact assessment, prior consultation (arts 35 and 36) and data breaches (arts 33 and 34). A strict relationship between security and risk management is also evident in the soft-law and co-regulatory instruments of the GDPR, such as the use of certification and codes of conduct (arts 40 and 42). See also Mantelero (n 6).

10 It should be noted that the Regulation also extends data security responsibility to data processors. A 'processor' is defined under the GDPR as someone who processes personal data on behalf of a controller.

11 See also PTJ Wolters, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7 *International Data Privacy Law* 2017 165–78; Kuner et al, 'The Rise of Cybersecurity and Its Impact on Data Protection' (2017) 7 *International Data Privacy Law* 73–75.

can be grouped into seven main areas in the field of data protection: (i) data minimization and data storage limitation; (ii) data confidentiality; (iii) risk assessment and security measures; (iv) data protection by design and by default; (v) regular assessment of the effectiveness of the security measures taken; (vi) notifications, reporting obligations and mitigation measures (data breaches); (7) business continuity, disaster recovery and resilience.

Regarding data minimization and data storage limitation, the GDPR requires controllers to limit the amount of data processed to the strictly necessary (data minimization). Moreover, personal data should not be retained for longer than required by the purposes for which they were collected, or for which they will be further processed (storage limitation). Controllers should therefore define the relevant data retention period and adopt systems to automatically delete the data after this period has expired.

From a cybersecurity perspective, a strategy focused on data minimization and storage limitation can help reduce the impact of data breaches resulting from cyberattacks or incidents.[12]

Regarding data confidentiality, the GDPR contains a set of provisions concerning access control and security,[13] based on a more general approach adopted by data protection law over the years which emphasizes the role of task distribution through the definition of roles and responsibilities of the entities involved,[14] a key organizational security measure.

Moreover, both controllers and data processors must put in place specific measures to ensure a level of security appropriate to the risk, including the confidentiality, integrity, availability and resilience of processing systems and services.[15]

These organizational measures should be implemented together with the technical ones. In particular, firms should adopt applications that allow them to create, approve, review and delete user accounts[16]. The use of log files is also an essential security measure, enabling the identification and tracking of user actions, and helping to identify potential internal and external attempts at system violation.

The Regulation does not stipulate a specific set of measures for this purpose, but many technologies for controlling access do exist, including in relation to network resources. One example of this are the servers known as Domain Controllers, which

12 See also A Mantelero and G Vaciago, 'Legal Aspects of Information Science, Data Science and Big Data', in M Dehmer and F Emmert-Streib (eds), *Frontiers in Data Science* (CRC Press 2017).

13 See below Table 1.

14 See also Recital 79 and art 28, GDPR.

15 See art 32, GDPR. The GDPR requires controllers and processors to, amongst other things, adopt appropriate security measures for protection against unauthorised access to systems (ie access control policies and systems), limiting employees and users' access to what is strictly necessary and restricting access to only those who have a legitimate reason to process or use it. See below Table 1. See also ENISA. *Handbook on Security of Personal Data Processing*. December 2017, 34. <https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing> accessed 30 January 2020.

16 See ENISA *Guidelines for SMEs on the Security of Personal Data Processing*. December 2016, 40. <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing> accessed 5 February 2020, which, among the different requirements of security systems, highlights 'the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity'.

normally use a management database to handle user authentication for access to machines and services.[17]

Moreover, in order to prevent data loss, destruction or damage, it is important to ensure server and database security, as well as network and communication security. Several measures can be taken in this respect. For instance, controllers should use anti-virus protection and malware detection systems and limit wireless access to the IT system. Monitoring traffic to and from the IT system is also important (eg through the use of Firewalls and Intrusion Detection Systems[18]).

The physical security of systems should also be taken into account to ensure a secure operating environment (for example, ID Badges for personnel and visitors accessing the premises of the organization, physical barriers, automatic fire suppression systems, continuous power supply, etc[19]).

Finally, hiding personal data and their interrelationships from plain view may also be useful to prevent data being acquired and misused by unauthorized actors. Among the measures that can be taken, the GDPR explicitly mentions pseudonymization and encryption.[20]

The last two areas of interaction between data protection and cybersecurity concern risk assessment (including security measures) and by-design and by-default approaches. Risk assessment represents an important tool for data processing design strategy, including the choice of the appropriate security measures to be implemented to ensure the protection of personal data and to safeguard the rights and freedoms of natural persons.

The GDPR adopts scalable modules, from a less structured assessment to a broad in-depth analysis,[21] with several obligations that have a procedural impact on the use of data, from the initial assessment phase to the concrete implementation of the outcome of the assessment. In this context, data processing monitoring[22] is another important obligation to ensure the scrutiny of data flows and the existing security measures.

The GDPR does not stipulate a specific set of security measures but rather requires data controllers and, where applicable, data processors, to adopt appropriate technical and organizational measures to protect personal data. They identify the appropriate measures taking into account the state of the art, the costs of implementation, the processing operations (nature, scope, context and purposes), and the risks of varying likelihood and severity for the rights and freedoms of natural persons.[23]

17 See, DQM GRC. *Essential Security Technologies for GDPR Compliance*, 6. https://www.dqmgrc.com/file/785/download?token=KuAoDE6C (5 December 2019, date last accessed).

18 See ENISA (n 16) 41.

19 ibid 46.

20 According to the GDPR, pseudonymization and encryption techniques are just a few examples of the measures that can be adopted by data controllers and processors to ensure data confidentiality. See Long W RM, *et al, European Union Overview. Privacy, Data Protection and Cybersecurity law Review* (5th edn, Law Business Research Ltd 2018), 14.

21 See arts 35 and 36, GDPR.

22 See art 30, GDPR.

23 See art 32, GDPR. In assessing the appropriate level of security, controllers must take into account, among other things, the risks that are presented by the processing, in particular from accidental or

The GDPR also provides some recommendations as to what type of security measures may be considered 'appropriate',[24] explicitly referring to specific technologies, such as pseudonymization and encryption,[25] and to procedural approaches,[26] including processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures already adopted.[27] Finally, adherence to an approved code of conduct or an approved certification mechanism may be used by controllers as a way to demonstrate compliance with the Regulation and conformity to security requirements.[28]

A broader perspective is then adopted in the provisions concerning the Data Protection Impact Assessment (DPIA), which goes beyond data security and takes a more holistic risk-based approach focusing on the impact of data use on the rights and freedoms of natural persons.[29] Controllers are thus required to assess the impact of the envisaged processing on data subjects, taking into account its necessity and proportionality, and identify the risks entailed by data processing for personal rights and freedoms. On the basis of this assessment, controllers must then take appropriate measures to address these risks.[30] Where the outcome of the DPIA indicates that the processing involves a high risk, which cannot be mitigated by the controller, the national data protection supervisory authority should be consulted.[31]

Based on the risk assessment, data controllers should put into place, both at the determination of the means of the processing and at the time of the processing itself, technical and organizational measures to implement data protection in an effective manner, to integrate the necessary safeguards with the processing and set any pre-existing configuration value or processing option in line with the principles of data minimization and purpose limitation (data protection by design and by default).[32]

unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

24 See art 32.1, GDPR.

25 See Long et al (n 20). See also Recitals 28, 83, GDPR.

26 See art 32.1.b (ongoing confidentiality, integrity, availability and resilience of processing systems and services) and 32.1.c (the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident) GDPR.

27 See art 32.1.d, GDPR.

28 See art 32.3, GDPR. See also Recital 77 and arts 24.3, 25.3.

29 See CD Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) *Computer Law & Security Rev.* 2020, <https://doi.org/10.1016/j.clsr.2020.105404>; R Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34(2) *Computer Law & Security Review* 279–88; A Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment' (2018) 34(4) *Computer Law & Security Review* 754–72. See also Preamble, Convention Cybercrime (ETS No 185), Council of Europe.

30 See arts 35.7 and Recitals 84 and 90, GDPR. See also art 29 Data Protection Working Party (n 8).

31 See art 36, GDPR.

32 See art 25, GDPR. See also EDPB. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, adopted on 13 November 2019. <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en> accessed 27 December 2019; L Jasmontaite *et al*, 'Data protection by design and by default' (2018) 4 *European Data Protection Law Review* 168–99; LA Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4 *Oslo Law Review* 105–20; D Le Métayer, 'Privacy by Design: A Matter of Choice', in S Gutwirth, Y Poullet, and P De Hert (eds) *Data Protection in a Profiled World* (Springer Netherlands 2010), 323–34. This attention to technology development to address data protection concerns through technological solutions has its roots in the Privacy Enhancing Technologies

Compared with the obligations in the first four areas of data protection relating to cybersecurity, the remaining three areas (regular assessment of the effectiveness of existing security measures; notifications, reporting obligations and mitigation measures; business continuity, disaster recovery, and resilience) are more procedural or sector-specific in nature.

Regarding assessment of security measures,[33] businesses should carry out vulnerability assessments and application and infrastructure penetration tests, but the GDPR does not specify any particular techniques for this purpose.[34]

More detailed provisions concern notifications and reporting obligations, in the event of security incidents (data breaches), including the consequent mitigation measures. The GDPR requires controllers to report personal data security breaches to the competent supervisory authority without undue delay, unless they are able to demonstrate that the breach is unlikely to result in a risk to the rights and freedoms of data subjects.[35]

Controllers must also communicate the data breach to the data subject if such an event is likely to result in a high risk to data subject's rights and freedoms.[36] Again in this case, the EU legislator emphasizes the security aspect. Communication is not required if controllers have implemented appropriate prior or subsequent technical and organizational measures to render the personal data unintelligible (eg adequate encryption) or to exclude high risks to data subjects' rights and freedoms.

As for the mitigation measures, controllers should adopt internal processes to prevent, detect and address personal data breaches. Examples of such measures include data flow and log analysers to detect any irregularities in personal data processing.[37] The GDPR also suggests using tools and technologies to limit the consequences of data breaches (eg tokenization and encryption).[38] From an organizational perspective, controllers should establish and document the main procedures to be followed in the event of a personal data breach to facilitate the overall handling of such incidents.

Moreover, controllers must keep an internal register of incidents and personal data breaches, detailing the event and subsequent mitigation action taken.[39] This

(PETs) developed since the '70s. See also European Data Protection Supervisor (EDPS). *Opinion 5/2018. Preliminary Opinion on privacy by design*, 31 May 2018, 3. <https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 1 February 2020.

33 See art 32.1.d, GDPR.

34 Examples of testing tools and services may include, inter alia: software to test connections to outside networks and look for gaps in configuration (vulnerability scanning) and ethical hacking (also called 'white hat' hacking). See, DMQ GRC (n 17) 11.

35 See art 33, GDPR.

36 See art 34, GDPR.

37 See, art 29, Data Protection Working Party. *Guidelines on Personal Data Breach Notification under Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, 12. <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> accessed 3 February 2020.

38 It should be noted that, even where data is encrypted, a loss or alteration can have negative consequences for data subjects if the controller has not implemented adequate backup procedures. Moreover, when backup procedures exist, the data breach might still have to be notified, depending on the length of time taken to restore the data from backup copies and the effect that a lack of availability has on individuals. See, art 29, Data Protection Working Party (n 37), 18.

39 See art 33.5, GDPR.

documentation will help controllers demonstrate their accountability and compliance with GDPR provisions.

Among the data security obligations, the GDPR also requires the adoption of measures to ensure data availability and recovery in case of loss or destruction resulting from a data breach (eg data backup and restore procedures).[40] More broadly, the GDPR aims to ensure the resilience[41] of the processing systems and services. Thus, controllers should take organizational measures to meet this requirement (eg disaster recovery plans and cyber-resilience strategies[42]) and adopt appropriate technological systems and tools to ensure business continuity (eg redundancy techniques).[43]

Summary of security obligations in the GDPR

The GDPR provides a set of security obligations concerning the protection of personal data which, directly or indirectly, underpin the development of cybersecurity strategies. This concerns a wide range of security applications that can be grouped into eight main areas, based on their correlation with GDPR principles. The following table shows this correlation between data protection principles, the GDPR provisions and the technical and organizational measures stipulated to implement them (Table 1).

THE PAYMENT SERVICES DIRECTIVE FRAMEWORK AND SECURITY OBLIGATIONS

The focus on the risk to personal data and the creation of an appropriate organizational and technological environment for the use of data are also the features characterizing the Payment Services Directive (PSD2),[44] where the goal of the EU legislator is, on the one hand, to benefit consumers by stimulating competition between Account Servicing Payment Service Providers (ASPSPs) and, on the other, to provide a robust harmonized legal framework across the EU.

This framework raises two new issues: (i) the transfers of consumers' personal data and (ii) the special cybersecurity obligations on the various players in the payment market.

With regard to the second issue,[45] payment institutions are required to provide specific information in their application for authorization to operate, among which:

40 See art 32.1.c, GDPR.

41 Resilience refers to the ability of the system to continue operating under adverse conditions, such as those that may result from a physical or technical incident and to the ability to restore such systems to an effective state.

42 See, IT Governance, Green paper. *Cybersecurity and business resilience* <https://www.itgovernance.co.uk/cyber-resilience> accessed 3 February 2020.

43 See art 32.1.b, GDPR.

44 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. OJ L 337, 23.12.2015, p. 35–127

45 See art 5, PSD2.

Table 1: GDPR

Rules and principles	GDPR	Technical and organizational measures
Data minimization	Recitals 28, 39, 83 Articles 5.1.c, 25.1, 32.1.a	**Organizational measures** • Identification of data strictly necessary for processing purposes **Technical measures** • Systems and services that minimize data collection and use of personal data
Data storage limitation	Recital 39 Article 5.1.e	**Organizational measures** • Definition of relevant data retention periods **Technical measures** • Systems for automatic periodic data deletion
Data confidentiality	Recitals 28, 39, 83 Articles 5.1.c, 5.1.f, 25, 32.1.a, 32.1.b, 32.1.4	**Organizational measures** • Security policy (ie access control policy, personnel roles and responsibilities, confidentiality and personnel training, resource management) • Records of processing activities **Technical measures** • Hiding personal data and their relationships (eg pseudonymization and encryption) • Access control to database and services (log files, applications to create, approve, review and delete user accounts, etc) • Server and database security/network and communication security (eg anti-virus protection, malware protection, monitoring traffic to and from the IT system) • Physical system security (eg ID badges, physical barriers, uninterruptible power supply)
Risk assessment and security measures	Recitals 84, 90 Articles 30, 32, 35	**Organizational measures** • Risk analysis and DPIA, including technical and organizational measures

(*Continued*)

Table 1: (continued)

Rules and principles	GDPR	Technical and organizational measures
Data protection by design and by default	Recital 78 Article 25	**Organizational measures** • Adoption of specific security requirements and procedures from the early stages of the development lifecycle • Procedures to integrate data protection safeguards into processing activities **Technical measures** • Special technologies to support privacy and data protection (PETs) (ie tools that encourage data minimization, anonymization or limitation of use, amongst other things)
Regular assessment of the effectiveness of the security measures adopted	Article 32.1.d	**Organizational measures** • Records of technical and organizational security measures taken **Technical measures** • Vulnerability and penetration testing (eg vulnerability scanning, ethical hacking)
Notifications, reporting obligations, and mitigation measures (data breaches)	Recitals 85, 86, 87 Articles 33, 34	**Organizational measures** • Procedures to immediately detect whether a personal data breach has taken place • Incident response plan **Technical measures** • Data flow and log analysers • Tokenization, encryption, etc.
Business Continuity, Disaster Recovery, and resilience	Article 32.1.b, 32.1.c	**Organizational measures** • Business continuity plan • Data restore procedures • Adoption of an effective cyber-resilience approach • Disaster recovery plan **Technical measures** • Backup techniques • Business continuity technologies (eg redundancy techniques)

- Description of the procedure in place to monitor, handle and follow-up any security incident or security-related customer complaint, including an incident reporting mechanism which recognizes the payment institution's notification obligations.[46]
- Description of the business continuity arrangements clearly identifying the critical operations, the contingency plans and the procedures to regularly test and review the adequacy and efficiency of such plans.

These provisions are coherent with the need to implement specific cybersecurity technical standards which requires, on the one hand, risk management, security readiness and incident response preparedness in reducing the risks and consequences of major cyber and physical events, including (i) an adequate corporate governance structure; (ii) security policies and incident response plans, procedures and toolkits; (iii) information sharing arrangements with government agencies and industry centres; (iv) table-top exercises; (v) third-party vendor contracts and management; (vi) insider threat programmes; and (vii) employee training programmes.

In the event of a cyber incident or major physical security emergency, the firm must have a comprehensive incident response plan in place to manage the full range of tasks. This should include (i) internal investigations; (ii) engagement with law enforcement and regulatory agencies; (iii) compliance with individual notification requirements and government reporting obligations; (iv) preparation for litigation and advice on data retention obligations; (v) public relations, employee communications and investor relations; (vi) responding to legal inquiries and preparing executives for hearings; and (vii) handling class action lawsuits, government enforcement actions and dispute resolution proceedings.

Moreover, all Member States must ensure that Payment Service Providers provide a scheme of appropriate mitigation measures and control mechanisms to manage operational and security risks.[47] They must also establish and maintain effective incident management procedures, which should include the detection and classification of major operational and security incidents.

The providers must also forward to the competent authority an updated and comprehensive assessment of the operational and security risks, either on an annual basis or at shorter intervals as determined by the competent authority. This requirement is obligatory in order to prevent incidents and ensure adequate awareness of the current risks.

Finally, the rules require the establishment, implementation and monitoring of the security measures, including certification processes. Where requested by the Commission, the EBA (European Banking Authority) will draft regulatory technical standards on the criteria and conditions for this process. Cooperation on this matter is promoted by the EBA, including the sharing of information among the competent authorities and between the competent authorities and the ECB (European Central Bank) and, where relevant, ENISA.

46 See art 96, PSD2.
47 See art 95, PSD2.

Regarding notification obligations, payment service providers must report any major operational or security incident, without undue delay, to the competent authority in the provider's home Member State.[48] If the incident may have an impact on the financial interests of its payment service users, the provider must promptly inform its users of the incident and any mitigation measures.

The national authority must report the incident to the EBA and the ECB and, after assessing its importance, to the relevant authorities in the Member State and, if necessary, to other authorities. The ECB and EBA, together with the national authority, must assess the relevance of the incident to other Union and national authorities and notify them accordingly. The ECB will notify the members of the European System of Central Banks on any issues pertinent to the payments system.

This notifications scheme is clearly designed to allow the competent authorities to take all necessary steps to protect the immediate safety of the financial system. National regulations also require providers to send the national authorities an annual report giving statistical data on fraud.

The EBA will issue specific guidelines on the classification of major incidents and how to assess their relevance.

The PSD2 Directive also contains provisions on authentication. Article 97 requires Member States to ensure that a payment service provider applies strong customer authentication when the payer interacts with the system to: (i) access their payment account online; (ii) make an electronic payment transaction; (iii) perform any action through a remote channel which may imply a risk of payment fraud or other abuses.

This is the provision that most emphatically shows how the new payments environment is focused on secure technological measures to prevent fraud and unauthorized access.

The Directive imposes several obligations on the EBA to provide payment service providers with technical authentication and communication standards, specifying: (i) strong customer authentication requirements; (ii) strong authentication exemptions; (iii) compliance requirements for security measures; and (iv) requirements for common and secure open standards of communication for the purpose of identification, authentication, notification and information. The EBA must also review and, where appropriate, update the regulatory technical standards in view of any innovation and technological developments.

For example, among the duties specifically provided by the Directive, the European Banking Authority's Guidelines (2017) set out the criteria and methodology to be used by payment services to classify an incident as major and therefore subject to mandatory notification to the competent authority in the Member State. Accordingly, the Financial Stability Board (FSB) specifies:

- mitigating operational risk from third-party service providers
- increasing cybersecurity measures, and
- monitoring macro-financial risk

as the three priority areas for international cooperation.

48 See art 5, PSD2.

Summary of security obligations in the PSD2 Directive

The Directive provides for the introduction of Third-Party Providers (PISPs and AISPs) as new payment services with permission to access users' accounts. This innovative system requires technologies that can guarantee protection of financial data to prevent the whole environment becoming insecure for both banks and non-bank institutions (see Table 2).

Recital 93 underlines the need to create a system in which the regulatory technical standards are compatible with the available technological solutions. The business model, whether based on direct or indirect access, must meet the data protection and security requirements laid down or described in the Directive or the regulatory technical standards.

The new environment provides several channels of communication for all players. Different kinds of communications must be designed to match the different types of information exchange and their various features.

The main categories of players specified by the Directive are the following:

- PISPs/AISPs and banks
- Different authorities of Member States
- National authorities and European organizations
- EBA and ECB.

The technologies to be adopted to meet the above requirements must be designed to prevent unlawful access to the data and information shared between the different players and between providers and authorities.

THE REGULATION ON ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR ELECTRONIC TRANSACTIONS IN THE INTERNAL MARKET (EIDAS REGULATION)

The eIDAS Regulation[49] is the legislative basis for electronic interactions between businesses, citizens and public authorities, improving the efficiency of online services and e-business transactions in the European Union. By providing a legal framework for the exchange of identity, this Regulation thus constitutes a further context where the interaction between personal data—in terms of digital identity and access to personal data through digital identity—and security can be examined in concrete terms, focusing on the role played by technical and organizational measures.

In this regard, one of the most important innovations of the Regulation is the distinction between Advanced Electronic Signatures (AdES)[50] and Qualified Electronic

49 Regulation (EU) No 910/2014 of the European Parliament and of Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

50 This is an electronic signature which meets the following requirements, set out in art 26 of the eIDAS Regulation: (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under her/his sole control; and (iv) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Table 2: PSD2 Directive

Rules and principles	PSD2	Technical and organizational measures
Risk assessment and security measures[a]	Recitals 91, 96 Articles 5.1.j, 95.1, 97	**Organizational measures** • Operational and security risk management framework (Security policy document) • Control model, to identify and manage operational and security risks **Technical measures** • Physical security (eg ID badges, physical barriers, uninterruptible power supply) • Access control (physical and logical access, strong controls over privileged system access) • Continuous monitoring and detection
Data protection (security) by design and by default	Recital 89	**Technical measures** • Secure technologies by design and by default should find solutions to common critical points (connectivity into banks, security fraud and liability, poor user authentication experiences, granting permissions)
Notifications, reporting obligations, and mitigation measures	Article 96 Article 5.1.f	**Organizational measures** • Appropriate processes and organizational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents • Reporting procedures **Technical measures** • Early warning indicators that should serve as an alert to enable early detection of operational or security incidents
Business Continuity, Disaster Recovery and resilience	Article 5.1.h	**Organizational measures** • Identify a range of different scenarios • Develop response and recovery plans, which should:

(*Continued*)

Table 2: (continued)

Rules and principles	PSD2	Technical and organizational measures
		• focus on the impact on the operation of critical functions, processes, systems, transactions and interdependencies; • be documented and made available to the business and support units and readily accessible in case of emergency; • be updated in line with lessons learned from the tests, new risks identified and threats and changed recovery objectives and priorities. • Governance arrangements and crisis communication plans • Procedures to verify the ability of staff and processes to respond adequately to the above scenarios
Certification process[b]	Article 95.3	**Organizational measures** • The Guidelines do not specify the requirements in relation to certification processes, or industry standards such as ISO 27001/22301; as such, no national authority requires such certification processes at present.
Annual report to the European Authority [c]	Article 96.6	**Organizational measures** • Member States shall ensure that payment service providers provide their competent authorities, at least on an annual basis, with statistical data on fraud relating to different means of payment. Those competent authorities shall provide the EBA and the ECB with this data in an aggregated form.

[a]EBA. *Final Report on Guidelines on Security Measures for Operational and Security Risks under PSD2* <https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf > accessed 1 February 2020 ('These Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that PSPs must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide').

[b]Source: EBA (n 49).

[c]Source: EBA. *Guidelines on Fraud Reporting under PSD2*. 2020 <https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2> accessed 1 February 2020.

Signatures (QES),[51] introduced in order to provide consistency across all EU member states in the way that documents can be signed.

Both AdES and QES prove the identity of the signer and are the equivalent to an ink signature. The difference lies in their acceptance by other EU Member States (ie states other than that of the trust provider). It is also significant that the Regulation specifies that an AdES cannot be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form or that it does not meet the requirements for qualified electronic signatures.

The eIDAS also introduces the recognition of electronic seals which are similar to signatures but can only be linked to legal persons and corporate entities. An electronic seal is data in electronic form, which is attached to, or logically associated with, other data in electronic form to ensure the latter's origin and integrity.[52]

The eIDAS Regulation establishes three levels of assurance for identification schemes that are directly proportional to their legal value[53]:

- Low Assurance, which provides limited confidence in the identity of the signer (eg this type of credential might only prove ownership of an email address).
- Substantial Assurance, which provides a limited degree of confidence in the claimed identity of a signer (eg to achieve this assurance level it is necessary to prove ownership of an email address and the identity of the signer).
- High Assurance, which provides a high degree of confidence in the claimed identity of a person. In addition to proving the person's identity, a high assurance credential might also prove legal representation of the organization(s) by the individual in question.

Whatever the assurance level, States who have notified an identity scheme become liable for it, as well as for the registration of the data operators, and any identity/authentication providers included in the notified scheme.

Moreover, for electronic signatures to pass the eIDAS qualifications they must be created using a Digital Certificate purchased from a 'trust services provider', such as a Certificate Authority (CA). It is important to note that the regulation allows national legislators to customize implementation but requires specific criteria to ensure a reliable system and a secure information regime.

To achieve an adequate security level for electronic identification means and trusted services, the Member State must provide the Commission with the following information:

- A description of the electronic identification scheme
- The applicable supervisory regime and information on liability
- The authority or authorities responsible for the electronic identification scheme

51 An advanced electronic signature is created by a qualified electronic signature creation device, and is based on a qualified certificate for electronic signatures

52 This kind of seal is similar, in its function, to the traditional business stamp and can be applied to an electronic document to guarantee the origin and integrity of a document.

53 See art 8 and Recital 16, eIDAS.

- Information on the entity or entities which manage the registration of the unique person identification data
- A description of how the requirements are to be met
- A description of the authentication mechanism
- Arrangements for suspension or revocation of either the notified electronic identification scheme or authentication or the compromised parts concerned.

The eIDAS Regulation requires a range of responses in the event of a security breach, in particularly notification of the competent authority and a remediation plan to contain the spread of the breach.[54]

First, where either the electronic identification scheme is breached or partly compromised in a manner that affects the reliability of cross-border authentication, the notifying Member State must, without delay, suspend or revoke that cross-border authentication or the compromised parts of it, and must inform the other Member States and the Commission.

Secondly, once the breach is remedied, the notifying Member State must re-establish cross-border authentication and promptly inform the other Member States and the Commission. If the breach is not remedied within three months of the suspension or revocation, the Member State must notify the other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Regulation also introduces common security standards shared by Member States[55] and the new role of the supervisory body, whose duty is to inform other supervisory bodies and the public of any breaches of security or loss of integrity.[56]

Trust service providers must comply with specific security requirements, specifically technical and organizational measures and notification of breaches.[57] Qualified and non-qualified trust service providers must take appropriate technical and organizational measures to manage the risks posed to the security of the trust services they provide. With regard to the latest technological developments, these measures must ensure that the level of security is commensurate with the degree of risk. Measures must be taken to prevent and minimize the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

Regarding notification obligations, qualified and non-qualified trust service providers must, without undue delay, but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies (eg the competent national body for information security or the data protection authority) of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider must also notify the natural or legal person of the breach of security or loss of integrity without undue delay. Where appropriate, in particular if a breach of

54 See art 10, eIDAS.
55 See art 12 and Recital 20, eIDAS.
56 See art 17, eIDAS.
57 See art 19, eIDAS.

security or loss of integrity concerns two or more Member States, the notified supervisory body must inform the supervisory bodies in other Member States concerned and ENISA.

The notified supervisory body must inform the public or require the trust service provider to do so, where it has determined that disclosure of the breach of security or loss of integrity is in the public interest. Once a year, the supervisory body must provide ENISA with a summary of any security breach or loss of integrity notifications received from the trust service providers.

Summary of security obligations in the eIDAS Regulation

The two key areas of cybersecurity covered by the eIDAS Regulation are the technical and organizational measures to manage risks and the notification of security incidents, with a view to furthering four main goals: identity verification and electronic transactions, market transparency, provider accountability and flexibility of government services.

The Regulation requires two different type of notification. The first is the description of the electronic identification procedures in each Member State. Here the Commission publishes a list of the electronic identification schemes notified in the Official Journal of the European Union. The second is the notification of security incidents, in line with the general direction of recent European regulation.

The supervisory body is also required to provide ENISA with an annual report of any security breach or loss of integrity notifications received from trust service providers.

The framework underlines the importance of ENISA, which crucially monitors the entire cross-border environment and activates proactive defences described in the following table (Table 3). Its EU-wide remit means it can adopt multiple layers of security protection to prioritize those entities most at risk of attack and minimize the harm caused by any incidents.

Rather than being focused on detection, the scope of eIDAS is primarily geared to monitoring incidents based on the observable cyber threats. This has led regulators to review the previous regulation, as data analytics and collection have come to play a bigger and bigger role in analysing threats, prediction modelling and detecting security incidents.

THE NIS DIRECTIVE FRAMEWORK AND SECURITY OBLIGATIONS

While it is true that the Payment Services Directive (PSD2) and eIDAS Regulation did not have an exclusive focus on security, the NIS Directive was specifically designed to regulate the security of Networks and Information Systems. Although the scope of this Directive is broader than data protection, as it covers both personal data and data relating to the network and information systems, it relies on the same technical and procedural approach that we discussed in the previous sections. At the same time, the NIS Directive contributes significantly to creating a safe environment for data processing and information sharing.[58]

58 See also Wolters (n 11).

Table 3: eIDAS Regulation

Rules and principles	eIDAS	Technical and organizational measures
Risk assessment and security measures	Article 19	**Technical measures** Authentication factors, which fall into the following categories: • Knowledge-based factors (eg PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to be known only to the subject) • Possession-based factors (eg asymmetric cryptographic (private) keys, where the private keys may be stored on dedicated hardware devices (eg smartcards), or software tokens, uniquely identifiable tokens (eg the SIM card of a cell phone) or devices with one-time-passwords, eg 'RSA-Tokens' or printed cards) • Biometric factors (eg fingerprints, palm prints, palm veins, face, hand geometry, iris, etc)
Data protection by design and by default[a]	Article 12.3.c	**Technical measures** • Software development has inspired the use of a catalogue of precise design patterns to develop solutions to known security problems. • Risk management frameworks and engineering objectives highlight a privacy risk model and three privacy system objectives (on top of the classic security objectives represented by confidentiality, integrity and availability): predictability, manageability and disassociability (US NIST).
Notifications, reporting obligations, and mitigation measures	Recitals 31, 38, 39 Article 19.2	**Organizational measures** • Notification can be of the user or by publishing the required information on the provider's website

(*Continued*)

Table 3: (continued)

Rules and principles	eIDAS	Technical and organizational measures
		depending on the nature of the breach, using applications or software to provide a document or fill in a form to notify providers of any incidents.
Business Continuity, Disaster Recovery, and resilience	Article 10.3 Article 24.2.h and 24.2.i	**Organizational measures** • Business impact analysis and threat analysis (to identify events that could cause an interruption of business operations and processes). • Following threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential business applications and processes. • All these activities must be performed with the full involvement of the owners of the business data and business processes, and using new technologies such as: risk management, vulnerability management, identification and prioritization of business processes and supporting applications, etc.
Certification process	Recitals 44 Recital 55	**Organizational measures** • Assessment of Standards related to eIDAS[b]: ENISA sets out aspects of qualified electronic signature creation devices (QSCD certification) and qualified trust services providers (QTSP supervision) showing how to combine the respective elements in line with the eIDAS requirements. **Technical measures** • ENISA[c] seeks to support standards CEN EN 419 241-2 and CEN EN 419 221-5:2018 so that they could

(*Continued*)

Table 3: (continued)

Rules and principles	eIDAS	Technical and organizational measures
		be referenced in an amended version of CID (EU) 2016/650.

Annual report to the European Authority	Article 19.3 (report to ENISA)	**Organizational measures**
		• The supervisory body must provide ENISA with an annual report on security breach and loss of integrity notifications received from trust service providers.
		
		Technical measures
		• Various technical measures should be developed to facilitate reporting on the vital infrastructure of the digital society, electronic communication networks and services:
		  • applications or open source software for quick and easy reporting
		  • technologies to classify annual incidents
		  • sets of capabilities for sector and industry clusters.

[a]Source: European Data Protection Supervisor (n 32).
[b]ENISA. *Assessment of Standards Related to eIDAS*. 2018 <https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas> accessed 1 February 2020.
[c]See (n 62).

European Union recognition that cybersecurity incidents might affect a large number of Member States led the EU legislator to improve European preparedness for cyber incidents through the NIS Directive,[59] which is addressed in particular to the essential services sector, comprising companies and organizations identified as either Operators of Essential Services (OESs) or Competent Authorities (CAs). It also applies to providers of network and information systems, which include all electronic communications networks, and any device or group of interconnected devices which are programmed to automatically process digital data or any data stored, processed, retrieved or transmitted by the above systems for the purposes of their operation, use, protection and maintenance.

The NIS Directive has four principal goals: (i) manage security risk; (ii) protect against cyberattack; (iii) detect cybersecurity events; and (iv) minimize the impact of cybersecurity incidents. Within this framework a crucial notion is that of risk, which

59 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.

is defined as 'any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems'.

With a view to raising the common security level of network and information systems across the EU, the NIS Directive: lays down obligations on all Member States to adopt a national strategy on network and information systems security; creates a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States and foster trust and confidence amongst them; creates a network of Computer Security Incident Response Teams (CSIRTs network) to further contribute to the growth of trust and confidence; establish security and notification requirements for operators of essential services and digital service providers; and lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs.

From an organizational perspective, the Directive provides a framework for strategic objectives and priorities on the security of network and information systems at a national level. It lists the significant elements that each Member State's national strategy must contain:

- The objectives and priorities of the NIS (network and information systems) security strategy.
- A governance framework to achieve these objectives and priorities, including roles and responsibilities for government bodies and other actors.
- Identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors.
- An indication of the education, awareness-raising and training programmes on the NIS security strategy.
- An indication of the research and development plans relating to the NIS security strategy
- An assessment plan to identify potential risks.
- A list of the various actors involved in the implementation of the NIS security strategy.

To fulfil these obligations, each Member State may request the assistance of ENISA in developing its national NIS strategy.

Each Member State's computer security incident response team (CSIRT) should be equipped with sufficient resources to effectively carry out its duties and have access to an appropriate, secure and resilient national communication and information infrastructure.[60] Member States must also ensure the effective, efficient and secure cooperation of their team in the CSIRTs network and may count on the assistance of ENISA in developing their national CSIRT.

Articles 11 and 12 define the Cooperation Group and the CSIRTs network, respectively, and their roles in promoting cooperation, exchange of information and trust and confidence among Member States. The Directive also underlines the importance of international cooperation,[61] with provisions allowing the EU to sign agreements with third countries or international organizations.

60 See art 9, NIS.
61 See art 13, NIS.

The Directive specifies security requirements, incident notification procedures and technical and organizational measures to manage security risks to network and information systems.[62] The EU legislator also requires Member States to ensure that operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the systems used to provide such services and guarantee their continuity, with the ensuing obligation on providers and operators to implement business continuity and disaster recovery plans.

Member States must ensure that operators of essential services promptly notify the competent authority or CSIRT of any incidents having a significant impact on the continuity of the services they provide. Notifications must include the information enabling the competent authority or CSIRT to determine the cross-border impact of the incident, if any. Notification must not entail greater liability for the notifying party.

There are three criteria in determining the significance of the impact: number of users affected by the disruption of the essential service, duration of the incident and geographical extent of the area affected.

Member States must ensure that digital service providers identify the security risks posed to the network and information systems used to offer their services and put in place appropriate and proportionate technical and organizational safeguards.

Regarding the state of the art of the measures, they must ensure a level of security of network and information systems appropriate to the risk, and take into account the following elements: security of systems and facilities, incident handling, business continuity management, monitoring, auditing and testing and compliance with international standards.

On the question of notification, Member States must ensure that digital service providers notify the competent authority or CSIRT, without undue delay, of any incident having a substantial impact on the service they offer within the Union. Notifications must include the information enabling the competent authority or CSIRT to determine the cross-border impact of the incident, if any. Notification must not entail greater liability for the notifying party.

In determining whether the impact of an incident is substantial, the following elements must be taken into account: number of users affected by the incident, duration of the incident, geographical extent of the area affected, extent of the disruption to functioning of the service and the extent of the impact on economic and societal activity.

Finally, both operators of essential services and digital service providers are required to implement a similar level of security, taking specific steps to prevent breaches of security and loss of integrity, and ensure consequent notification.

Summary of security obligations in the NIS Directive

In fulfilling their NIS Directive obligations, operators of essential services and digital service providers are expected to engage in a best-efforts risk management process designed to identify, assess and address any threats to service that might entail economic and social damage (see Table 4).

62 See art 14, NIS.

Table 4: NIS Directive

Rules and principles	NIS Directive	Technical and organizational measures
Risk assessment and security measures	Recital 49 Article 14.1, 14.2 and Article 16.1 and 16.2	**Technical measures** • Communication (email) risk assessment (Domain Keys Identified Mail, Sender Policy Framework, Domain-based Message Authentication, Reporting and Conformance) • Software management • Access control • Authentication factors
Data protection (security) by design and by default	N/A	
Notifications, reporting obligations, and mitigation measures	Article 9. 4 Article 14.3 and 14.4 Article 16.3 and 16.4	**Organizational measures** • Providers and operators must immediately report significant disruptions to the National Agency and the reporting obligations must have no adverse effect on correcting the disruption. **Technical measures** • Technologies supporting notification and reporting obligations must: (i) adopt alerting systems; (ii) gather information on incidents; (iii) provide automated completion of notifications using pre-established NIS elements (number of users affected, duration of incident, geographic spread, extent of disruption to service, impact on economic and social activity).
Business Continuity, Disaster Recovery, and resilience	Recitals 69 Article 14.2 and Article 16.1.c	**Organizational measures** • Operators and providers must ensure cyber-resilience, implementing business continuity management measures such as: • cyber risk and vulnerability management

(*Continued*)

Table 4: (continued)

Rules and principles	NIS Directive	Technical and organizational measures
		• incident response team • alternative resources in the event of crisis • backup systems.
Certification process	N/A	
Annual report to the European Authority	Article 11.3.j	**Organizational measures** • The Commission will examine, on an annual basis, the summary reports referred to in the second subparagraph of Article 10 (3) (notifications). **Technical measures** • Adequate resources to assist in handling information necessary for the report • Strong authentication channels to collect and store data on incidents to be reported • Structural support to target and keep strictly confidential data and information on incidents • Secure channel for information sharing with the Commission

The NIS Directive underlines the importance of notification and international coordination and creates new institutional cybersecurity bodies, such as the Cooperation Group to facilitate strategic cooperation and exchange of information between Member States, and the CSIRTs.

COORDINATED ANALYSIS OF THE LEGAL INSTRUMENTS EXAMINED

This analysis of the differing legal sources making up the current EU framework on data protection and cybersecurity found the Europe Union's regulatory approach to be generally favourable. This conclusion is borne out by the table that follows, showing the results of the coordinated analysis carried out in the previous sections (Table 5).

It is clear that the GDPR provides a general framework, defining and stating the main binding principles for data use and data security, such as data minimization, storage limitation and data confidentiality, that shape the entire edifice.

On these criteria, as well as risk assessment, by-design approach, reporting obligations, and the certification process, the GDPR takes a principles-based approach that

Table 5: Common core

Rules and principles	GDPR	PSD2	eIDAS	NIS
Data minimization	Systems and services that minimize data collection and use of personal data.			
Data storage limitation	• Data retention limitations • Pseudonymization • Encryption • Access control • Server and database security • Network and communication security • Automatic periodic data deletion			
Data confidentiality	• Security policies • Records of processing activities • Physical security			
Risk assessment and security measures	• Risk analysis • DPIA	• Operational and security risk management framework	• Use of authentication factors (Knowledge-based	• Communication (email) risk assessment (Domain Keys Identified Mail,

(*Continued*)

Table 5: (continued)

Rules and principles	GDPR	PSD2	eIDAS	NIS
	• Technical and organizational measures	• Control model • Physical security • Access control • Continuous monitoring and detection	factors, possession-based factors, private keys) • Use of inherent factors	Sender Policy Framework, Domain-based Message Authentication, Reporting and Conformance) • Software management • Access control • Authentication factors
Data protection by design and by default	• Adoption of specific security requirements and procedures from the early stages of lifecycle development • Procedures to integrate data protection safeguards into processing activities • Specific technologies able to support privacy and data protection (PETs)	Secure technologies by design and by default (data minimization, pseudonymization, encryption, privacy-oriented users' profiles settings).	Use a catalogue of specific design patterns to develop solutions to known security problems.	
Regular assessment of the effectiveness of the security measures adopted	• Records of technical and organizational security measures adopted • Vulnerability and penetration testing (eg			

(*Continued*)

Table 5: (continued)

Rules and principles	GDPR	PSD2	eIDAS	NIS
	vulnerability scanning; ethical hacking)			
Notifications, reporting obligations, and mitigation measures (data breaches)	• Appropriate procedures to establish immediately whether a personal data breach has taken place • Incident response plan • Data flow and log analysers • Tokenization; encryption, etc.	• Early warning indicators • Processes and organizational structures to ensure the consistent and integrated monitoring, handling and follow-up of operational or security incidents • Procedure for reporting	• Applications or open source software for quick and easy reporting • Technologies to classify annual incidents	• Mandatory report to the National Agency in case of significant disruptions • Adopt alerting systems • Information collection on incidents • Provide information on security issues • Automatization of notification systems
Business Continuity, Disaster Recovery, and resilience	• Business continuity plan • Data restore procedures • Adoption of an effective "cyber- resilience" approach • Disaster recovery plan • Backup techniques • Technological measures to ensure business continuity	• Identify a range of different scenarios • Develop response and recovery plans	• Business impact analysis and threat analysis • Recovery time	• Cyber-resilience and business continuity • Cyber risk and vulnerability management • Incident response team • Alternative resources to use in case of crisis • Backup systems

(*Continued*)

Table 5: (continued)

Rules and principles	GDPR	PSD2	eIDAS	NIS
Certification process	Voluntary certifications issued by certification bodies (Article 43 GDPR) or by the competent Supervisory Authority.	• No specific requirements for certification or default industry standards	Qualified electronic signature creation devices (QSCD certification) and qualified trust services provider (QTSP supervision).	• No specific legal requirements for certification or default industry standards, but ENISA recommends[a] European Data Protection Certifications, such as relevant ISO standards including ISO 17021 or ISO 27006
Annual report to the European Authority		Member States must ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities must provide the EBA and the ECB with such data in an aggregated form.	The supervisory body must provide ENISA once a year with a summary of any security breach or loss of integrity notifications received from the trust service providers.	• Adequate resources to assist in handling information necessary for the report • Strong authentication channels to collect and store data on incidents to be reported • Structural support to target and keep strictly confidential data and information about incidents • Secure channel for information sharing with the Commission

[a]ENISA, *Recommendations on European Data Protection Certification*. 2017 <www.enisa.europa.eu>at_download>fullReport> accessed 1 February 2020.

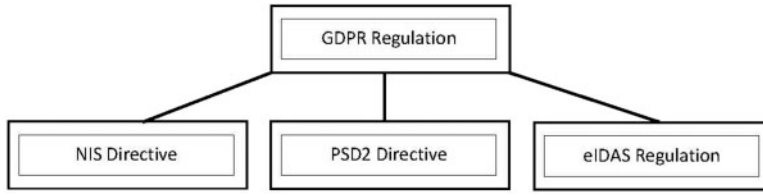

Figure 1: Relationship with the various regulations.

is crucial in establishing a basic paradigm. However, this paradigm needs to be further elaborated through examination of the other regulations, with a more technology-based and context-specific focus.

All these legal instruments call for the development of appropriate cybersecurity and data security technologies, either explicitly or implicitly, as illustrated in Table 5 below. At the same time, the framework provided by these different legal sources is not a patchwork, but a coordinated harmonious model, in which similar technologies are required by differing regulations to address issues related to a common core based on five central pillars: risk-based approach, by-design approach, reporting obligations, resilience and certification schemes.[63]

Another aspect to be considered is the importance given to supply chain security and the consequent relationship between the four European regulations. GDPR Article 28 highlights the requirements that should be met by all service providers, while the other instruments contain provisions addressing specific sectors: essential services, banking, electronic communications and online transactions. The relationship between the various regulations is represented in genealogical form (from genus to species) in the figure above (Figure 1).

This conclusion is bolstered by the obligations on data controllers defined in GDPR Article 24.1, which sees the nature, scope, context and purposes of processing, and the varying likelihood and severity for the rights and freedoms of natural persons, as parameters for the implementation of 'appropriate technical and organizational measures' by controllers. The same notion of appropriateness appears again with reference to data processors needing to provide sufficient guarantees to implement appropriate technical and organizational measures.[64]

The GDPR does not define appropriateness, but refers to it as a factor that entails a balancing test,[65] as demonstrated by Recital no. 84 which points out a direct

63 See also Title III, Regulation (EU) 2019/881 on ENISA (European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act); ENISA. *Bolstering ENISA in the EU Cybersecurity Certification Framework*. 2019. <https://www.enisa.europa.eu/publications/bolstering-enisa-in-the-eu-cybersecurity-certification-framework> accessed 1 February 2020.

64 See art 28.1, GDPR.

65 See eg the notion of appropriateness in the contest of GDPR sanctions ('as a standalone corrective measure, or in combination with other measures in article 58, such aggravating or attenuating circumstances may help to choose the appropriate measures by tipping the balance in favour of what proves more effective, proportionate and dissuasive in the given case', art 29 Data Protection Working Party. *Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679*. 2017, 13

relationship between appropriate measures and risk assessment.[66] A measure is therefore deemed appropriate if it addresses the risks involved in a given case of data processing.

Appropriateness is a contextual notion, dependent on the nature of the data processing, so that its meaning cannot be circumscribed by the GDPR, which is general in character. For application of provisions in context we must turn to the three sector-specific instruments, the NIS Directive, PSD2 Directive and eIDAS regulation. Here the appropriateness of the required measures is framed in terms of the risks and available responses in the various contexts. GDPR Article 28 places on service providers operating in these fields the general obligation to adopt more specific and tailored solutions.

This contextualization of the GDPR obligations, however, does not compromise the security requirement. On the contrary, it clearly reveals the uniformity of approach of the EU legislator to the issues of data security and cybersecurity in the business environment. It highlights the existence of a common thread running through the entire framework which clearly revolves around a few key clusters of security measures and procedures, as outlined in the following table.

CONCLUSIONS

This article presents a functional analysis of some of the main binding instruments of the regulatory framework behind cybersecurity and data security, departing from the traditional approaches to legal commentary to focus on the relationship between the formal requirements of EU legislation and the technical means of implementing them. This approach has enabled us to identify the key elements of the various legal provisions critical to data security and cybersecurity strategy.

This analysis has also revealed the interconnections between the different legal instruments and the technology-focused backbone of the EU approach in this area. We highlight the unique nature of the EU framework which fosters fundamental rights through technology, boosting the development of data protection and cybersecurity research based on a by-design approach which safeguards individual rights and societal interests in the digital economy.

We demonstrate that the legal requirements, and the EU framework more generally, provide a very favourable environment for the development of EU cybercrime policies and strategy and, from a technological perspective, help to guide this process along specific axes in terms of cybersecurity research and development.

In particular, a coordinated analysis of the different legal sources has identified three main elements in the EU's regulatory approach: a balance between principles-based provisions and technical rules, a variety of technological solutions seen by law as crucial to achieving the EU objectives in data protection and data security, and a clustering of the entire legal framework around five core elements (risk assessment, by-design approach, reporting obligations, resilience, and certification schemes).

<https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> accessed 1 February 2020).

66 See Recital no 84 GDPR ('The outcome of the assessment should be taken into account when determining the appropriate measures to be taken').