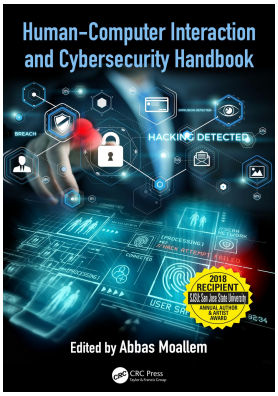

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Impact of recent legislative developments in the European Union on information security

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-15
Gerald Quirchmayr
Published online on: 24 Oct 2018

chapter fifteen

Impact of recent legislative developments in the European Union on information security

Gerald Quirchmayr

Contents

15.1 Privacy and critical information infrastructure protection regulation: Background

Privacy and information security are some of the core concerns in the design, development, and operation of IT systems. With recently published solid evidence from Europol [2016 and 2017; Internet Organised Crime Threat Assessment (IOCTA)], the size and intensity of the problem facing Europe is well documented. It was in May and June 2017 that waves of serious attacks based on exploits leaked after the intrusion of secret service systems (EternalBlue 2017) have again shown the need for a concerted action against these now very dangerous attacks (National Audit Office 2017). With new legislation in both areas, privacy protection [General Data Protection Regulation (GDPR), Regulation (European Union [EU]) 2016/679] (European Parliament and Council of the EU 2016a), and critical infrastructure security [NIS Directive, Directive (EU) 2016/1148] (European Parliament and Council of the EU 2016b), the EU is now countering the growing danger on a strategic level. These two pieces of legislation are a direct consequence of the European cybersecurity strategy (EU 2013), which paved the way for a now far more integrated approach.

This new legislation introduces a much needed basis for information sharing about cyberattacks and reporting obligations on incidents and updates the by now partially obsolete European privacy legislation that came into effect in 1995 (Directive 95/46/EC) (European Parliament and Council of the EU 1995). One of the very significant differences is that the new privacy legislation, which will become effective in 2018, is now a directly applicable law, a major step forward from previous guidelines that were aimed only at the harmonization of laws in member states of the EU. For system developers and system operators, the resulting competitive advantage is that from May 2018, they will have only one central privacy law to be compliant with for all member states in the EU,

the world's largest single market. The much younger European network and information security legislation still takes form in a directive (Directive (EU) 2016/1148). Considering the many different interests and approaches of member states in the fields of national security and national defense, a joint European strategy and umbrella legislation in the domain of cybersecurity is therefore also a major improvement that only a few decades ago would have been unthinkable. With national interests and economic needs of member states and of the EU as a whole being reflected in the new legislation, a successful implementation of the legislation can be expected. This chapter looks at the two central pieces of legislation, the GDPR [Regulation (EU) 2016/679] and the NIS Directive [Directive (EU) 2016/1148] primarily from a system development and information technology (IT) operations perspective.

15.2 GDPR [Regulation (EU) 2016/679]

The GDPR was introduced as the successor of the European privacy legislation introduced in 1994 (Directive 95/46/EC) to address new technological developments, such as cloud computing, Internet of things (IoT), and smartphones, and to establish a new adequate basis for technology applications such as social media that were not yet on the horizon in 1994 but are a major economic and societal factor today. As a compromise is reached between privacy advocates, government agencies, and industry, the regulation is primarily aimed at providing a balanced and workable solution and does consequently receive continuing criticism from privacy advocates (Fielder 2017).

The EU data protection reform was adopted by the European Parliament and the European Council on April 27, 2016. The European Data Protection Regulation will be applicable as of May 25, 2018, and replace the Data Protection Directive. The regulation is grouped (EU Info 2017) into introductory chapters (Chapters 1 and 2), covering general provisions and principles, and Chapters 3–5 covering the rights of the data subject, obligations of controller and processor, and the transfers of personal data to third countries or international organizations.

Independent supervisory authorities, cooperation and consistency; remedies, liability, and penalties; provisions relating to specific processing situations; delegated acts and implementing acts; and final provisions are regulated in Chapters 6–11.

Within these chapters, the rights of the data subject; obligations of controller and processor; transfers of personal data to third countries or international organizations; and remedies, liability, and penalties have received special attention.

Obligations regarding the safeguarding of personal information are specified in Chapter 4—Controller and Processor—Section 2—Security of Personal Data. Article 32—Security of Processing—contains a list of obligatory organizational and technical measures to be taken. As this article contains the primary obligations for system developers and operators, the full text is shown in Box 15.1.

A risk-based approach and adequate encryption and pseudonimization of personal data are the major new obligations introduced by Article 32. The requirement of regular testing, regular assessment, and evaluation of security measures is now made explicit.

While already well-established rights of individuals, such as the confidentiality of personal data, continue to be protected, the right to erasure ("right to be forgotten") in Article 17 and the right to data portability in Article 20 represent significant new challenges for system developers and operators.

It is, however, Article 25, Data Protection by Design and by Default, which has introduced the necessity to rethink system design and development whenever personal data are involved.

BOX 15.1 ARTICLE 32: SECURITY OF PROCESSING

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
   a. the pseudonymisation and encryption of personal data;
   b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   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;
   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall 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 he or she is required to do so by Union or Member State law.

While in the past, it was rather typical to retrofit IT security safeguards, they now have to be considered as a core requirement guiding the system design and development process.

As can be directly derived from the preceding text, the newly introduced legal obligations will lead to a very significant increase in terms of additional requirements and system design principles. Apart from design and development, Article 25 will also change the way in which systems dealing with personal data operate. (The controller shall implement appropriate technical and organizational measures for ensuring that by default, only personal data, which are necessary for each specific purpose of the processing, are processed.)

The obligatory data breach notification comes in two forms, Article 33—Notification of a Personal Data Breach to the Supervisory Authority—and Article 34—Communication of a Personal Data Breach to the Data Subject. A personal data breach means a breach of security leading to the destruction of, loss of, alteration of, unauthorized disclosure of, or access to personal data. This means that a breach is more than just losing personal data. Notifying the relevant supervisory authority of a breach becomes obligatory where such a breach is likely to result in a risk to the rights and freedoms of individuals. If unaddressed, such a breach is likely to have a significant detrimental effect on individuals—for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage [see ICO (2017)].

Article 35—Data Protection Impact Assessment—will have a significant consequence in the form of a privacy risk assessment having to be performed in the feasibility study stage of every IT project. Especially considering agile programming techniques, this will result in a major change of processes in terms of slowing down system development. Together with the principle of data protection by design and by default (Article 25), this legal requirement should ensure that privacy protection is adequately taken care of from the early stages of a project on.

Regulations governing the transfer of personal data to third countries or international organizations are laid out in Articles 44–50. The general principle for transfers sets the basis, followed by rules regulating transfers on the basis of an adequacy decision, transfers subject to appropriate safeguards, binding corporate rules, transfers or disclosures not authorized by Union law, derogations for specific situations, and international cooperation for the protection of personal data.

Penalties being imposed for violations of the guideline were discussed widely, because consequences can now be quite severe, since especially Article 83-4 ("Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher") introduces a very credible deterrent against violations.

This new privacy legislation has already led to a rethinking of privacy protection as an essential aspect of system design and development. While introducing new requirements (e.g., privacy by default) that certainly lead to higher development costs, it also leads to a higher level of system security. Given the recent sophisticated attacks, these obligations do reflect, however, only the growing threats and might soon be viewed as a very welcome guide to counter them. When applied by developers to system design beyond the protection of personal data, they might in a very positive way contribute to finally achieving the goal of designed-in, built-in security by default. How much such a general redesign of system development is already in the context of critical information infrastructures is addressed in the following description of the NIS Directive.

15.3 Directive on security of network and information systems (Directive (EU) 2016/1148)

With the Cybersecurity Strategy of the European Union (EU 2013) setting the stage for a better coordinated and more integrated approach to cybersecurity, the second strategic legislation to be passed was the NIS Directive in 2016 [Directive (EU) 2016/1148]. "Recognizing that network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market," the directive aims at providing a harmonized approach "responding effectively to the challenges of the security of network and information systems therefore requires a global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers," setting a minimum standard across the EU. Higher levels of protection than required by the directive are of course highly welcomed by the document.

In (7) of the preamble, the applicability of the directive is stated as follows:

> To cover all relevant incidents and risks, this Directive should apply to both operators of essential services and digital service providers.

> However, the obligations on operators of essential services and digital service providers should not apply to undertakings providing public communication networks or publicly available electronic communication services within the meaning of Directive 2002/21/EC of the European Parliament and of the Council (1), which are subject to the specific security and integrity requirements laid down in that Directive, nor should they apply to trust service providers within the meaning of Regulation (EU) No 910/2014 of the European Parliament and of the Council (2), which are subject to the security requirements laid down in that Regulation.

The governing principles are laid out in Article 1—Subject Matter and Scope (Section 2).

> 2. To that end, this Directive:
>
> a. lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;
> b. creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
> c. creates a computer security incident response teams network ("CSIRTs network") in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
> d. establishes security and notification requirements for operators of essential services and for digital service providers;
> e. lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

It is Article 1, Section 2 (c), which implements the vision of giving computer security incident response teams (CSIRTs)/computer emergency response teams (CERTs) a central role in the fight against cyber threats, as envisaged in EU (2013) (Figure 15.1):

The security and notification requirements for operators of essential services and for digital service providers established in (d) should assure a common minimal level of protection and information sharing regarding critical information infrastructures.

Article 2—Processing of Personal Data—references to the relevant EU legislation. Article 3—Minimum Harmonization—introduces the principle of a minimal level of security that should be achieved in all member states of the EU. A guideline for the "identification of operators of essential services" is provided by Article 5 of the directive.

Chapter II—National Frameworks on the Security of Network and Information Systems—defines the obligation of member states, respectively:

The high importance of ENISA, the European Network and Information Security Agency, as hub for knowledge and information exchange, is underlined in the preamble and in several articles of the directive and especially in Article 12.

Chapter IV—Security of the Network and Information Systems of Operators of Essential Services—introduces the minimal obligations to be fulfilled, with Article 14—Security Requirements and Incident Notification—being the central point of reference

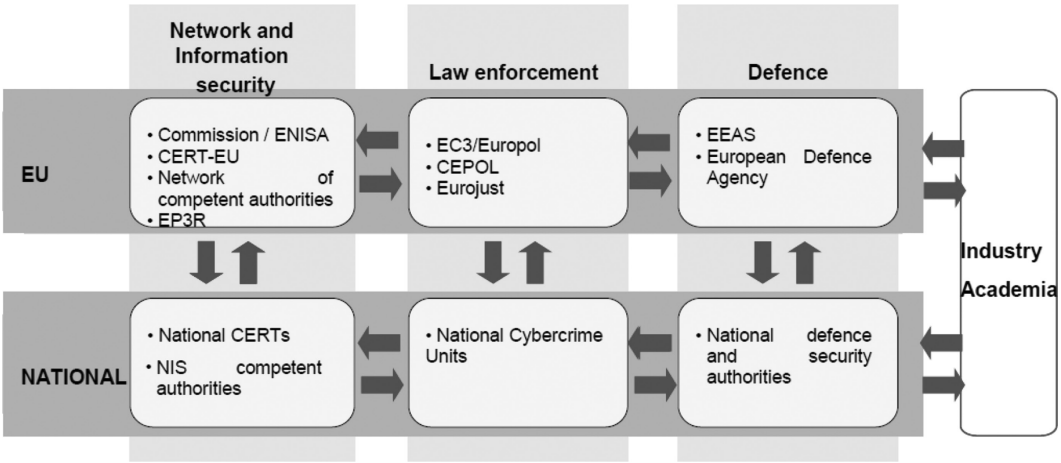

Figure 15.1 Role of CERTs/CSIRTs. CEPOL: European Union Agency for Law Enforcement Training; CERT-EU: Computer Emergency Readiness Team for the EU institutions, agencies and bodies; EC3: European Cybercrime Centre; EEAS: European External Action Service. (Extracted from EU, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions*: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, http://ec.europa.eu/information_society/newsroom/cf//document.cfm ?doc_id=1667, 2013.)

for the safeguards and measures to be implemented. Article 15—Implementation and Enforcement—defines who Article 14 is to be acted on.

From an IT technology point of view, Chapter V—Security of the Network and Information Systems of Digital Service Providers—should be used as a core guidance. While not being surprising in its content, Article 16 introduces quite challenging requirements for system operators (Box 15.2).

The full implementation of the preceding requirements can be expected to result in substantial costs for system development and operations. With Article 16 stating the obligations in rather general terms, a more detailed implementation guideline will be needed. This guideline will most probably come in the form of national NIS legislation.

Incidents leading to reporting duties are defined in Article 16, Section 4:

> 4. In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:
>   a. the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
>   b. the duration of the incident;
>   c. the geographical spread with regard to the area affected by the incident;
>   d. the extent of the disruption of the functioning of the service;

BOX 15.2 ARTICLE 14: SECURITY REQUIREMENTS AND INCIDENT NOTIFICATION

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:
   a. the security of systems and facilities;
   b. incident handling;
   c. business continuity management;
   d. monitoring, auditing and testing;
   e. compliance with international standards.

e. the extent of the impact on economic and societal activities. The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.

Article 16, Section 5, regulates notification duties in the case of outsourced services:

> Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.

Chapter VI—Standardisation and Voluntary Notification—is aimed at achieving a standardized communication and information exchange and provides a legal basis for nonobligatory information sharing (voluntary notification). This voluntary notification will be especially helpful in unclear situations where new emerging cyberthreats have to be dealt with and in the early stages of a massive cyberattack, when first indicators of compromise become visible, but the damage resulting from an attack is still below the threshold that would lead to an obligatory notification.

With creating a network of trusted CSIRTs and national hubs, establishing standardized information exchange, and strengthening the position of ENISA, the NIS Directive is an essential step toward securing the European cyberspace. It finally gives government agencies, CSIRTs, and law enforcement the long overdue legal basis for a much needed EU-wide closer and better structured cooperation. Focusing on critical infrastructures this directive also adheres to the principle of concentrating available European resource on essential efforts.

15.4 Expected impact on information security and privacy management

The expected impact of the introduction of the GDPR [Regulation (EU) 2016/679] is a more comprehensive harmonization of privacy protection across the EU. New and emerging technologies as well as new business models should be covered by the GDPR. While it fully satisfies all desires neither of privacy activists nor of industry, it is a solid compromise that gives society and economy a good basis to address the needs of privacy-related governance issues in cloud computing; social media; smart mobile devices; smart infrastructures, such as the smart power grid and smart metering; and the abundance of privacy issues related to IoT technology.

The NIS Directive [Directive (EU) 2016/1148] is aimed at establishing a common minimal level of critical information infrastructure protection in all member states of the EU. With the central role attributed to CSIRTs and the establishment of dedicated national hubs that serve as focal points for information exchange and cooperation in the case of a major cyberattack against Europe, a new infrastructure for more effectively countering cyberthreats will be introduced. The obligation to report major incidents is expected to lead to a much better and much faster coordinated reaction in case an attack starts spreading across the EU. Improved situation awareness, better and earlier information about developing threats and attacks, and the ability for a coordinated reaction is aimed at leading to a safer European cyberenvironment. The new European privacy and security legislation can be considered as a milestone for securing critical infrastructures, services, and processes across the EU while at the same time updating privacy legislation to enable it to cope with new digital business models and new technologies. The legislative process started by Directive 95/46/EC has now entered a next level, acknowledging the continuously increasing importance and growing dependence of the economy and of society as a whole on information and communication technology-based (cyber-) infrastructures.

References

Burgess, M. (2007) Everything you need to know about EternalBlue – the NSA exploit linked to Petya, WIRED, 28 June 2017, https://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch.

ENISA. https://www.enisa.europa.eu/; accessed 2018-05-23.

EU (2013) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions*: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667.

EU Info (2017) *Structured Overview of General Data Protection Regulation GDPR*, https://gdpr-info.eu/.

European Parliament and Council of the EU (1995) Directive 95/46/EC of the European Parliament and Council of the EU of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031–0050.

European Parliament and Council of the EU (2016a) 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).

European Parliament and Council of the EU (2016b) The Directive on security of network and information systems (NIS Directive), https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

Europol (2016) *The 2016 Internet Organised Crime Threat Assessment (IOCTA)*, European Police Office, 2016, ISBN 978-92-95200-75-3; ISSN 2363-1627, available on https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

Europol (2017) *The 2017 Internet Organised Crime Threat Assessment (IOCTA)*, European Police Office, 2017, available on https://www.europol.europa.eu/sites/default/files/.../iocta2017.pdf.

Fielder, A. (2017) *New EU Data Protection Laws: Ok, but a Tremendous Missed Opportunity with Possible Threats Looming*, https://www.privacyinternational.org/node/689.

ICO (2017) *Guide to the General Data Protection Regulation (GDPR)*, https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/.

National Audit Office (2017). National Audit Office, Report by the Comptroller and Auditor General Department of Health Investigation: WannaCry cyber attack and the NHS, HC 414 SESSION 2017–2019 25 APRIL 2018, published 24 October 2017.