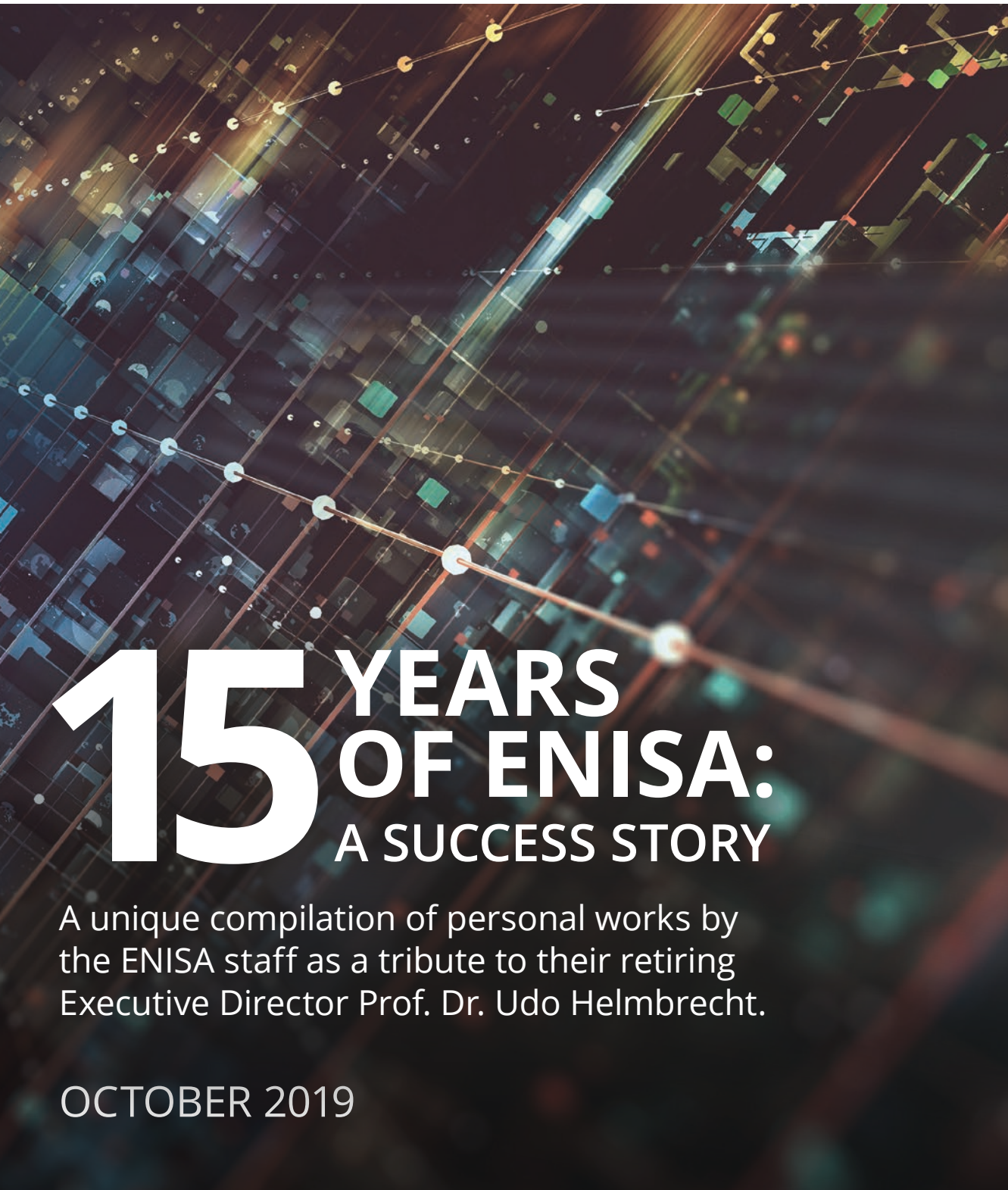
EUROPEAN UNION AGENCY FOR CYBERSECURITY



15 YEARS OF ENISA: A SUCCESS STORY

A unique compilation of personal works by the ENISA staff as a tribute to their retiring Executive Director Prof. Dr. Udo Helmbrecht.

OCTOBER 2019

CONTACT

For contacting ENISA please use the following details:
press@enisa.europa.eu
Info@enisa.europa.eu
website: www.enisa.europa.eu

LEGAL NOTICE

COPYRIGHT NOTICE

Print ISBN 978-92-9204-300-1 doi:10.2824/381557 TP-02-19-613-EN-C
PDF ISBN 978-92-9204-302-5 doi:10.2824/669379 TP-02-19-613-EN-N

15 YEARS OF ENISA: A SUCCESS STORY

A unique compilation of personal works by the ENISA staff as a tribute to their retiring Executive Director Prof. Dr. Udo Helmbrecht.

OCTOBER 2019

TABLE OF CONTENTS

10. SECURITY MEETS DATA PROTECTION: FROM RISK MANAGEMENT TO SYSTEMS ENGINEERING

By Athena Bourka, Prokopios Drogkaris

10.1 INTRODUCTION

When discussing security and the protection of personal data, there is typically a perception that these two concepts are distinct, albeit sometimes related or even conflicting. Indeed, the notion of 'balancing' security and data protection (or privacy as a broader concept) is not unusual ([222]), e.g. in debates around access to (online) data for security purposes, as if there is a trade-off between 'safeguarding the internet' and 'protecting individual rights'. This standpoint stems from the (also) typical perception that security (e.g. of the internet or of the cyberspace) is of broader societal value, while data protection is a rather personal matter. Importantly, security is considered to have a more tangible technical side, when data protection is mainly a legal issue mandated by the General Data Protection Regulation (GDPR) [11] or other similar regimes and depicted in long (and often complicated) policies, terms or contractual clauses ([223]).

However, as recent large-scale personal data breaches have shown, the reality is far more complex. The numbers speak for themselves: only within 2018, 1244 personal data breaches took place and over 440 million data records were compromised [12], including those of Facebook ([224]), Google+ ([225]) and Marriott Starwood Hotel ([226]). These only followed several serious breaches of previous years, such as those of Yahoo! ([227]), Uber ([228]), Equifax ([229]), eBay ([230]), and Ashley Madison ([231]), to name just a few. When analysing this new online phenomenon, some interesting observations can be made.

222 See also: Charles D. Raab, 'Designing Privacy and Security: Beyond the Technical Perspective' in ENISA's Annual Privacy Forum 2015, https://2015.privacyforum.eu/programme/presentation-raab

223 See e.g. analysis on the cost of privacy policies in: https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf

224 https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach

225 https://www.wired.com/story/google-plus-bug-52-million-users-data-exposed/

226 https://www.pcworld.com/article/3324609/marriott-starwood-hotel-data-breach-faq.html

227 https://www.theguardian.com/technology/2017/oct/03/yahoo-says-all-of-its-3bn-accounts-were-affected-by-2013-hacking

228 https://us.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html

229 https://www.nytimes.com/2017/10/02/business/equifax-breach.html

230 https://www.reuters.com/article/us-ebay-password/ebay-asks-145-million-users-to-change-passwords-after-cyber-attack-idUSBREA4K0B420140521

231 https://www.independent.co.uk/life-style/love-sex/ashley-madison-hacking-accounts-married-man-exposes-cheating-website-infidelity-rick-thomas-a7529356.html

Personal data in an emerging threat landscape

Clearly, the value of personal data in the online world has significantly increased. This is due to the increase of the (re)usability of these data. Reports have shown that personal data obtained through cyberattacks are utilised to generate new attacks and to support different types of illegal and/or criminal activities [13]. Moreover, personal data misuses can go beyond the breach of individual rights to compromise broader societal functions, even that of the democratic elections ([232]). They can do so by targeting large groups of people or just single individuals ([233]).

At the same time, due to the increased value of personal data and new technological possibilities, the (cyber) threats and risks are evidently elevated. Aside the standard 'old-school' attacks, organisations are experiencing today more sophisticated incidents, such as for example ransomware attacks. While the insider threat is still prominent, external malicious intent is increasing [14], including that of activist nature.

Yet, despite the criticality of the assets and the level of the risks, the (cyber) security measures used for the protection of personal data appear to be inadequate or inefficient. Although human error is even now the cause of many incidents, many serious data breaches, as those mentioned above, have occurred due to 'poor security measures' ([234]), such as for example undiscovered bugs and exploitable vulnerabilities. What do all these mean in practice?

The crossroads of security and personal data protection

Simply put, security and personal data protection are increasingly interlinked.

In the emerging threat landscape, data protection cannot be seen as an obscure legal concept anymore: data breaches are real and so are their millions of victims. At the same time, security cannot succeed its scope if it does not practically embed the protection of personal data: 'poor security measures' are not an option today in the cyberspace and beyond.

Both security and data protection are vital individual values, while being at the same time essential collective goods, without which societies cannot flourish ([235]). Security and data protection are eventually becoming the two sides of the same coin. It is, thus, critical, instead of their 'balancing', to start discussing their convergence.

Scope and structure of the paper

Following the aforementioned discussion, in this paper, we focus on the close link between security and data protection and explore the main needs as to their convergence, by analysing the specificities of personal data security (Section 2). To this end, we argue that information security management needs to go hand in hand with the assessment of data protection risks (Section 3). We discuss that security engineering needs to embrace the notions of privacy and data protection by design (Section 4). We finally seek to derive some conclusions for a future way forward (Section 5). While doing so, we also present the

232 See e.g. the relevant Facebook Cambridge Analytica case: https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data

233 See e.g. the Whatsapp spyware vulnerability case: https://www.theguardian.com/technology/2019/may/13/whatsapp-urges-users-to-upgrade-after-discovering-spyware-vulnerability

234 See for example analysis for the Marriott breach in: https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers

235 See also in: https://2015.privacyforum.eu/programme/presentation-raab

long-standing contribution and work of ENISA in this important field.

10.2 UNDERSTANDING PERSONAL DATA SECURITY

It is not difficult for one to defend that data protection is included in the very notion of information security, defined by ISO/IEC 27000:2018 as the '*preservation of confidentiality, integrity and availability of information*' (also known as the 'CIA triad') [15]. Personal data is one type of information and, consequently, falls directly under the aforementioned protection goals. The case is the same with regard to the more controversial notion of 'cybersecurity' ([236]), defined by ISO/IEC 27032:2012 [16] as the '*preservation of confidentiality, integrity and availability of information in the Cyberspace*' ([237]), which in fact extends the information security CIA paradigm to the special characteristics of the fully digitised and hyper-connected 'cyberspace' environment. Quoted often as 'the oil of the digital economy' ([238]), personal data undoubtedly form an integral (and, as discussed earlier, increasingly valuable) part of the cyberspace and, as a result, of cybersecurity.

While the protection of personal data falls under the definition of (information or cyber) security, security clearly also forms an integral part of personal data protection by (legal) definition. Indeed, the General Data Protection Regulation (GDPR) [11], apart from providing specific security obligations to data controllers ([239]), introduces for the first time security as one of the key principles relating to personal data processing. In particular, article 5(1)(f) GDPR states that personal data shall be '*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*'. As mentioned in ENISA's guidelines for the security of personal data processing [17], this evolution, security as a principle, puts security at the core of data protection together with other established data protection principles (e.g. lawfulness, fairness, purpose limitation, accuracy, etc.).

If, as discussed above, data protection is part of security and security is a data protection principle, it becomes apparent that these two concepts are strongly interlinked, at least at a conceptual level. However, as also recognised in ENISA's 2018 workshop report on security of personal data processing ([240]), bringing security at the level of a principle in data protection requires to foster a relevant security culture among the data controllers and to provide reflections on new security paradigms
(e.g. 'functional' security) that go beyond the traditional 'defensive' security.

In order to do so, it is essential for security to embrace the very nature of personal data, as well as the specificities that this nature brings to their protection.

236 See relevant discussion in: https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

237 Cyberspace is defined in ISO/IEC 27032:2012 as '*the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*'.

238 See for example in: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/

239 GDPR article 3(7): ' the natural or legal person, public authority, agency or other body which, alone or jointly with others, defines the purposes and means of the processing of personal data...'.

240 https://www.enisa.europa.eu/events/ws_personal_data_processing/

Exploring the nature and specificities of personal data

Starting from its GDPR definition (article 4(1)), personal data means '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'. GDPR recital (26) further explains that in order to determine whether a natural person is identifiable, account should be taken of '*all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*'. Following the aforementioned provisions, we can derive some principal characteristics of personal data, which are also paramount as to their protection.

Clearly, a critical parameter with regard to personal data is the level of identifiability of data subjects, which is highly dependent on the particular context of the processing of personal data, i.e. the specific conditions and circumstances under which data are being processed. Indeed, even the simple case of an individual's name can vary significantly: while a very common family name will not be sufficient to identify someone (i.e. to single someone out) from the whole of a country's population, this might become possible if the name is combined with other data, such as for example telephone number or email address [18]. In addition to this, the possibility of both direct, as well as indirect identification of the data subjects needs to be taken into account. As outlined in ENISA's report on data pseudonymisation [19]: '*This aspect is especially relevant to the use of online and mobile services, where a multitude of device and application identifiers are utilised (by the device/service/application providers) to single out specific individuals (i.e. the users of the relevant devices or applications).*'

Moreover, as the nature of personal data is highly context-based, it is also strongly dependant on the possibility to combine different types and/or amounts of information about the same individual. In other words, the value of a single piece of personal data increases when combined with other pieces of data for the same individual. Importantly, even if a certain piece of data would not constitute personal data under a specific context, its combination with other data about the same person might finally lead to the inference of personal data under a different context. Undeniably, several studies in the field have shown ([241]) that data inference (intended or unintended) has become one of the most prominent threats for personal data in the cyberspace today. The possibilities of machine learning and big data analytics play a central role in this. As discussed in ENISA's report on privacy by design in big data [20], '*it is feasible by combining various allegedly non-personal data to infer information related to a person or a group*', while, at the same time, '*the combination of anonymised datasets and advanced analytics can lead to re-identification of a person by extracting and combining different pieces of information*'. The use of multiple online identifiers, as well as data accumulated from sensors and (often uncontrolled) third party software (e.g. in the area of mobile apps), only adds to this serious issue [21].

On top of the previous points, a concluding fundamental aspect of the nature of personal data is simply the fact that they relate to natural persons. As such, any misuse of these data will have direct impact on those persons, which may cause them any type of physical,

241 See relevant discussion in: https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

material or non-material damage, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, heath impact, deprivation of rights, etc. This aspect, depicted in GDPR as the risk to 'the rights and freedoms of data subjects' [242], is in fact key to all the elements discussed so far. In order to properly address it in practice, it is indispensable not only to shift the assessment of the 'typical' security risks towards the highly contextual nature of the personal data (and the natural persons concerned), but also to integrate the procedures that can provide adequate information and control to those natural persons over their data. The latter, referring to the so-called data subjects' rights in GDPR, while not being a security issue per se, needs to be supported by adequate security mechanisms as well.

Extending the remits of security to personal data protection

Following the analysis so far, it appears that personal data security needs to extend the remits of the 'traditional' information security towards these special requirements of personal data. If this is not properly done, the protection would simply not be adequate. The security provisions in GDPR aim at exactly defending this line.

In particular, article 32 GDPR states that the controller *'taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals',.. 'shall implement appropriate technical and organisational 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 systems and services processing personal data; (c) the ability to restore the availability and access to 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 organisational measures for ensuring the security of the processing.'*

Analysing this provision, it becomes once more apparent that personal data security, while following the classic risk-based and CIA-based information security paradigm, introduces a new perception of risks towards the 'the rights and freedoms' of data subjects. Following this new perception, the technical and organisational measures for personal data security go also beyond the conventional understanding of information security (or cybersecurity) measures. Pseudonymisation and anonymisation techniques are examples of this extension, so are several other categories of privacy enhancing technologies (PETs) ([243]), such as e.g. Attributed Based Credentials (ABCs), encryption, anonymous communication, privacy preserving computations, as well as transparency & control mechanisms [22].

Understanding and incorporating these elements to standard security practices is fundamental to the protection of personal data. Convergence of security and data protection can, thus, only be achieved by integration: data protection requirements should form part of security risk management frameworks; PETs should become central elements of IT systems design.

In the following two sections, we discuss these two important dimensions by referring to relevant ENISA's work in these fields.

242 See also recital 75 GDPR.

243 A well-known definition of PETs was provided in [13] as follows: '*Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system.*'

10.3 EXTENDING SECURITY RISK MANAGEMENT TO PERSONAL DATA PROTECTION

IT security risk management is the process of identifying, quantifying, and managing the IT security risks that an organisation faces. Security risk assessment is at the heart of this process, followed by risk treatment, acceptance and communication. Typically, an information security risk is obtained through the combination of the likelihood that a threat materialises and the impact that a potential such incident may have for the organisation. Well-known standards, such as ISO/IEC 27005:2018 [24] and NIST 800-39 [25], have contributed towards relevant methods, tools and practical implementation ([244]).

As discussed earlier, personal data security is strongly risk-based. Still, a personal data security risk management system needs to adapt to the specificities of personal data. Evidently, as a first point, in the context of the risk assessment, the impact needs to be considered towards the individuals (and their rights and freedoms), hence taking a different angle from the classic security risk assessment. The scale is not necessarily relevant towards this end, e.g. the impact may be high even if the number of affected persons is low. In addition, possible secondary effects may also need to be considered (e.g. when assessing possible impacts of a personal data breach). Moreover, after the evaluation of risks, the risk management process also varies from typical security risk management.

For example, risk acceptance would not be possible in cases where risks to individuals are concerned. In addition, risk treatment would need to integrate privacy enhancing technologies, e.g. technologies reducing the identifiability of data subjects (and not necessarily qualifying under the general CIA protection technologies).

244 For more information, see: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management

ENISA's framework for personal data security risk management

Following these ideas and previous work in field [26] [27], ENISA proposed in 2016 a framework that supports organisations (Small and Medium Enterprises — SMEs) in assessing the personal data security risks and subsequently adopting security measures [17] (Figure 14).

As shown in Figure 14, ENISA's proposed framework comprises of five steps. The starting point (Step 1) is the definition (by the organisation, i.e. data controller) of the data processing operation and its context, which is fundamental for understanding the boundaries and specificities of the personal data processing. Based on this understanding, the evaluation of the impact to the rights and freedoms of data subjects follows (Step 2), as shown in Table 1. This is a qualitative approach that takes into consideration several contextual parameters, such as the type and volume of personal data, the criticality of the processing operation, special characteristics of the data controller and/or the data subjects, as well as the level of identifiability of data subjects.

The next step (Step 3) in ENISA's framework is the analysis by the controller of the threats related to the data processing environment and their likelihood (threat occurrence probability). Although this is also a qualitative process, it is performed with the help of specific questions guiding the controller through the assessment. After evaluating the impact and the threat occurrence probability, the final evaluation of risk is possible (Step 4), as shown in Table 2 below. The final step (Step 5) of the whole exercise is the selection of appropriate security measures by the controller. This is done per risk level with the use of a traffic-light system

Figure 14. Overview of ENISA's framework on personal data security risk assessment

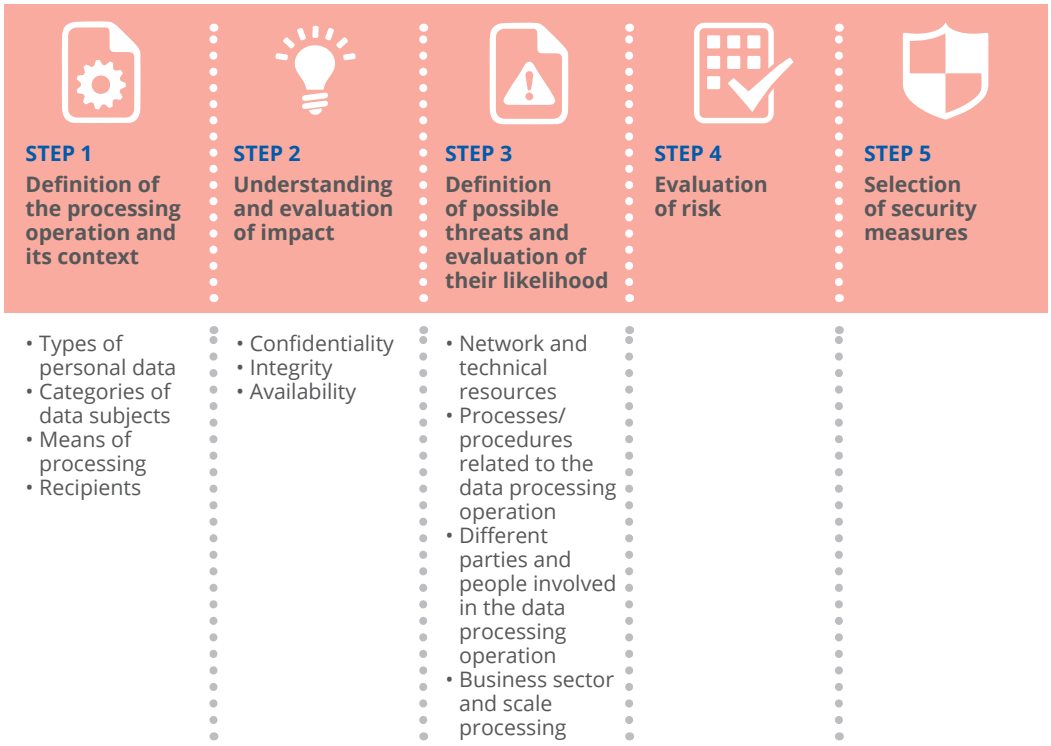


Table 1. Levels of impact to the rights of freedoms of data subjects

LEVEL of impact	Description
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Table 2. Evaluation of risk

		IMPACT LEVEL		
		Low	Medium	High/ very High
Threat Occurrence Probability	Low			
	Medium			
	High			

Low Risk Medium Risk High Risk

(low: green, medium: yellow, high: red). The measures follow the categorisation given in ISO/IEC 27001 [28] and ISO/IEC 27002 [29] with extensions covering specific requirements for data protection.

In order to interpret and practically demonstrate the aforementioned methodological approach, ENISA in 2017 published a handbook with specific use cases on personal data security risk assessment [30]. The use cases were focused on standard processing operations of a typical SME (human resources, customers' management/ marketing, safety and security, contractors/ service providers' management), as well as specifically on healthcare service providers and educational institutions.

Moreover, in 2018 ENISA published guidelines on well-established security practices for the protection of personal data, in particular in the fields of access control and authentication, incident handling and personal data breaches, logging and monitoring, server and database security, as well as workstation security [31]. Recognising the prominent role of pseudonymisation in personal data security, ENISA also published an overview of relevant techniques and use cases, together with an analysis of the role of pseudonymisation in the context of GDPR [19].

Challenges in personal data risk management

While the aforementioned ENISA's work, as well as other similar initiatives in the field ([245]) practically work towards the conjunction of security and data protection, there are yet several challenges in the field of security and personal data risk management.

Certainly, as outlined in ENISA's 2018 security of data processing event ([246]), organisations are lacking knowledge and experience, while the integration of data protection in established risk assessment frameworks, (that organisations usually follow) is generally missing. The need of guidance, tools and training for controllers is urgent for this purpose. So is the need for investing in the broader scope of privacy and data protection engineering at the very early stages of IT system design and throughout their whole lifecycle. Supporting the implementation of privacy and data protection by design is essential to this end.

245 See for example, the tool for data protection impact assessment issued by the French DPA, CNIL, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

246 https://www.enisa.europa.eu/events/personal-data-security/personal-data-security

10.4 EXTENDING SECURITY ENGINEERING TO PRIVACY AND DATA PROTECTION

Security by design is a core concept in information security, which refers to the embedding of security requirements early in the design and development process of IT systems and services. Obviously, such an approach can greatly enhance the suitability and efficiency of adopted security measures, making security a core aspect of the design and development process (rather than an auxiliary function). Different approaches towards security by design can be found in the literature. For example, in the area of software engineering, the OWASP development guide ([247]) defines a number of security by design principles, such as: minimise attack surface area, establish secure defaults, least privilege principle, defence in depth principle, fail securely, separation of duties, etc.

Privacy by design, initially introduced as a term in 1995 by the Ontario Privacy Commissioner [32], expands the notion of security by design into the embedding of privacy measures and privacy enhancing technologies (PETs) into the design of systems and services. Data protection by design, for the first time introduced as a legal obligation for controllers in GDPR, follows the same rationale. Indeed, article 25 GDPR mandates that the controller shall '*implement appropriate technical and organisational measures [...] which are designed to implement data-protection principles'.* This shall be done '*both at the time of the determination of the means for the processing and at the processing itself*'. In addition, the same article provides for the use of data-protection-friendly default settings (data protection by default).

247 https://www.owasp.org/index.php/Security_by_Design_Principles

Considering once again the conjunction of security and data protection, it is obvious that 'traditional' security engineering approaches, while highly important, are not enough to implement data protection principles in each particular personal data processing scenario. As also shown in [21] in the specific area of mobile apps, although the resolution of security issues could protect from several privacy violations, many data protection challenges would not be covered, e.g. data minimisation or the exercise of data subjects' rights. In order to practically approach the aforementioned issue, two different dimensions need to be considered: on one hand, the definition of privacy and data protection by design methodologies, which can be incorporated into existing security engineering approaches; on the other hand, the development and further adoption of PETs towards the definition of the state-of-the-art in this field.

Defining privacy by design methodologies

On the methodological side, researchers, as well as policy-makers have been actively working for several years towards the 'translation' of privacy and data protection requirements into technical implementation measures. ENISA in its 2014 report on privacy and data protection by design [22] presented two different (but interlinked) approaches to this topic: the data protection goals and the privacy by design strategies. The notion of data protection goals, proposed by [33] refers to the three security protection goals of unlinkability, transparency, and intervenability, which extend the CIA triad, but shift the perspective to the individual and the specific nature of personal data. The privacy by design strategies [34] aim at preserving certain privacy goals (Table 3); they are linked to privacy design patterns and can be implemented with the use of specific PETs. The idea of privacy strategies was also explored in ENISA's 2015 report on privacy by design

Table 3. Privacy by design strategies [24]

	Privacy by design strategy	Description
1	Minimise	The amount of personal data should be restricted to the minimal amount possible (data minimisation).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever personal data is processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controller must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

in big data [20], where these strategies were extended to the phases of big data analytics and mapped to relevant implementation solutions.

Although the aforementioned methodologies are significant steps for integrating privacy and data protection in the high-level objectives of security engineering, digging deep into the development ecosystem is equally vital. For example, in the area of mobile apps, as ENISAs relevant study argues [21], given the prominence of agile methodologies, it is salient to support research and development of scalable methodologies for data protection by design, e.g. by extending the agile Secure Development Lifecycle (SDL) ([248]) to address privacy and data protection requirements. Importantly, it is necessary to work towards the definition of a repository of PETs that can support practical implementation.

248 See in: https://www.microsoft.com/en-us/SDL/Discover/sdlagile.aspx

Analysing the state-of-the-art in PETs

With a view to contribute towards the definition of state-of-the-art in PETs, ENISA has worked over the years on methodologies and tools that can support the assessment of the maturity of PETs and the privacy protection that they offer. By doing so, not only vertical (technical) criteria should be considered, which are inherent to the functionality of the different tools, but also horizontal criteria that address broader (and sometimes less evident) parameters influencing privacy and data protection, such as for example the issue of software maintenance or usability aspects. To this end, in its 2015 readiness analysis for the adoption and evolution of PETS [35], ENISA proposed a methodology that can provide comparable information on the maturity of different PETs, by assessing their readiness and their quality on the basis of objective criteria (Figure 15).

Figure 15. An overview of ENISA's PETs maturity level evaluation

Idea--	Idea-	Idea^0	Idea+	Idea++
Research--	Research-	Research^0	Research+	Research++
PoC--	PoC-	PoC^0	PoC+	PoC++
Pilot--	Pilot-	Pilot^0	Pilot+	Pilot++
Product--	Product-	Product^0	Product+	Product++
Outdated--	Outdated-	Outdated^0	Outdated+	Outdated++

While the aforementioned methodology was generic enough to cover all possible types of PETs (and of different maturity levels), ENISA's PETs control matrix issued in 2016 [36] aimed at providing an assessment framework with both generic, as well as application-specific criteria that can be used for the assessment of specific types of PETs (Table 4).

As also discussed in the previously quoted work of ENISA, the notion of state-of-the-art in PETs (and in security technologies in general) comes with many challenges. Indeed, the assessment of PETs (and its trustworthiness) depends greatly on the chosen modalities, e.g. the identity of the evaluator (e.g. expert assessment versus self-assessment), the technical depth of the assessment, as well as the target audience (e.g. developers versus end users). For this reason, the definition of the state-of-the-art cannot be the work of one single entity but should rather be supported by the broader privacy and data protection community (so as to remain viable and neutral). There are already initiatives that contribute towards this direction, such as for example the EDPS IPEN network ([249]). Still, new governance models need to emerge, together with best practices and examples that can best demonstrate the applications of specific security technologies in certain data processing fields. Such models could develop towards the idea of an observatory of PETs, practically supporting the interlinking of security and personal data protection.

10.5 CONCLUSIONS AND WAY FORWARD

In this paper, we argued that security and data protection are closely interlined and it is, thus, essential to work towards their convergence. There is one answer to this demand: rethinking security in a way that it meets the needs of personal data. Our focus was on two different but strongly related dimensions to this end: on one hand, the extension of the 'traditional' security risk management towards personal data protection; and on the other hand, the integration of privacy and data protection by design in security engineering. This discussion is continuously emerging and there are several interesting ideas in this respect ([250]). Considering the previous analysis and the existing solutions, in this Section we derive some key conclusions for the way forward in personal data security.

249 https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

250 See also proceedings of the ENISA's Annual Privacy Forum published, https://privacyforum.eu

Table 4. ENISA's PETs control matrix — overview of generic and specific criteria

Pets assessment framework				
Specific criteria		**Generic criteria**		
Secure messaging tools	End-to-end encryption	Maturity and stability	Privacy policy implementation	Usability
	Client-Server Encryption			
	Security of stored Data			
	Authentication			
	Anoymoys communication			
Virtual private networks	Identity protection			
	VPN encryption			
	Side effects			
Anonymizing networks	Anonymiy protection			
	Encryption			
	Side effects			
Anti tracking tools	Blocking			

Firstly, in order to integrate data protection requirements into security frameworks, there is a need for re-engineering of the very notion of security. In order to do so, practical methodologies and tools are of high importance, taking especially into account that data protection should fit into the existing security frameworks, rather than creating new frameworks only for data protection. This last -often overlooked parameter- is critical as to the viability and efficiency of relevant frameworks.

Secondly, it is important to stress that many of the (security) technologies that would qualify for the protection of personal data (PETs) have been already available since many years: personal data security is, therefore, rather a matter of implementation, rather than of technological development per se. This needs to be considered in correlation with the risk-based approach of GDPR, meaning that the notion of the state-of-the-art (of security technologies) may be different in different sectors and under different levels of risks. It is, hence, necessary to work towards use cases and examples that can define what can really work in practice (and what cannot work), supporting data controllers and creating in this way new security models for the protection of personal data.

Thirdly, when defining frameworks and tools for personal data security and engineering, it is critical to respect the characteristics of the underlying ecosystems under which personal data are processed, and the relevant actors therein. If this aspect is omitted, data protection becomes only a high level objective, rather than a 'real' issue with tangible technical solutions. This means in practice that engineers and developers need to be involved with (and understand) data protection as well, aside managers and policy-makers. It also means that evolving methods of systems development need to be considered (e.g. agile

development) in the context of the security and privacy engineering.

Lastly, as outlined in ENISA's relevant study [37], privacy standards can also be an emerging area that can help the integration of privacy and data protection requirements in IT systems, although a lot of work is still needed, both at a conceptual, as well as at implementation level. Closely related to this, the area of certification, gaining increasingly importance, both in cybersecurity ([251]), as well as in data protection ([252]), is one more field where synergies in early steps could greatly help convergence.

251 As mandated in the EU cybersecurity certification framework under the EU Cybersecurity Act soon to come into effect, see in: https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity

252 Articles 42 and 43 GDPR.

Athena Bourka works at ENISA as a cybersecurity Expert in the European Union Agency for Cybersecurity (ENISA). Since 2015, she is also ENISA's Data Protection Officer (DPO). Before joining ENISA, Athena had been working for over 10 years as a privacy and security expert in the Hellenic Data Protection Authority and the European Data Protection Supervisor (seconded national expert). Athena has also worked in the past in the areas of healthcare security and environmental information systems, both in the private and public sector. She has studied electrical and computer engineering and holds a PhD on information ęsecurity from the National Technical University of Athens.

Dr Prokopios Drogkaris is an Expert in Network and Information Security at the European Union Agency for Cybersecurity (ENISA) in the areas of Privacy and Data Protection, Cybersecurity Certification and Trust Services. He holds a Diploma in Information and Communication Systems Engineering from the University of the Aegean, Greece, and an MSc in Information Systems from City University London, UK and a Ph.D. in Privacy and Security in e-Government Information Systems from the Department of Information and Communication Systems Engineering, University of the Aegean, Greece. He worked as a postdoc researcher within the University of Piraeus, at the Department of Digital Systems. Previously, he was involved in several EU funded research projects in the greater area of Information Security within the Hellenic Ministry of Citizen Protection and he held teaching assistant positions in higher education institutions. He is the author of several scientific publications and served as a member on program and organizing committees at International and European scientific conferences.

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

Publications Office
of the European Union