Guidelines for SMEs on the security of personal data processing

DECEMBER 2016

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups 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. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use pets@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank Ms. Georgia Panagopoulou (Hellenic Data Protection Authority) and Mr. Giuseppe D'Acquisto (Italian Data Protection Authority) for their advice and support throughout the preparation of this report.

ISBN 978-92-9204-209-7, DOI 10.2824/867415

Table of Contents

Executive Summary

In May 2015 the European Commission (EC) published its 'Digital Single Market Strategy for Europe'[1], outlining 16 legislative and non-legislative initiatives designed to create a single market in digital goods and services across the European Union. As part of this Strategy, the Commission drew attention to facilitate access to online markets, strengthen digital networks and boost the digital transformation of Small- and medium-sized enterprises (SMEs) which represent 99% of all businesses in the EU[2]. In order to also support the Single Market dimension of data protection, the EC proposed in 2012 a uniform set of rules to ensure a high level of data protection for individuals and promote legal certainty and consistency to all businesses across EU.

The General Data Protection Regulation (EU) 679/2016 ('GDPR') will be, as of 25 May 2018, the main data protection legal framework in EU directly applicable to all Member States, repealing the current Data Protection Directive 95/46/EC. Currently, businesses in the EU have to deal with 28 different data protection laws. This fragmentation is a costly administrative burden that makes it harder for many companies, particularly SMEs, to access new markets. The new rules are expected to bring benefits of an estimated €2.3 billion per year, at a European Level[3,4].

One of the core obligations for all businesses, including SMEs, acting either as data controllers or data processors, in GDPR is that of the security of personal data. In particular, according to GDPR security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk). Even if this risk-based approach is not a new concept only a few specific privacy risk assessment frameworks have been presented, focusing principally on the evaluation of risks to personal data and adoption of relevant security measures. While big companies have the possibility to respond to and appropriately implement these frameworks, SMEs do not always have the necessary expertise and resources to do so. Indeed, it is in many cases difficult for SMEs to comprehend the specificities of the risks associated with personal data processing, as well as to assess and manage these risks following a formal methodology[5]. This can put on harm's way the personal data processed by SMEs, hindering at the same time compliance of SMEs with the GDPR legal obligations.

On this basis and as part of its continuous support on EU policy implementation, ENISA undertook a study to support SME's on how to adopt security measures for the protection of personal data, following a risk-based approach. In particular, the objectives of the study were to facilitate SMEs in understanding the context of the personal data processing operation and subsequently assess the associated security risks. Based on that the study also proposes possible organizational and technical security measures for the protection of personal data, which are appropriate to the risk presented. These measures can be adopted by SMEs in order to achieve compliance with GDPR.

[1] https://ec.europa.eu/priorities/digital-single-market_en
[2] https://ec.europa.eu/growth/smes_en
[3] http://ec.europa.eu/justice/data-protection/files/4_strenghten_2016_en.pdf
[4] http://ec.europa.eu/justice/data-protection/document/factsheets_2016/data-protection-factsheet_01a_en.pdf
[5] Information security and privacy standards for SMEs: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport

On top of the aforementioned work, a number of challenges were also identified at a broader EU level and respective conclusions were drawn for all involved stakeholders, as follows:

No *one-size-fits-all* approach

GDPR provision for a risk-based approach is horizontal as there are not exemptions or light weight approaches based on the organization size, availability of recourses and capabilities. Similar to larger organizations, SMEs have to identify the level of risk, depending on nature, scope, context of processing along to the types and volumes of data processed.

Guidance Needed

SMEs are not fully acquaint to the perception of risk from the personal data perspective and they could benefit from a more guided approach that will bridge the gap between the legal provisions and their understanding and perception of risk. Such guidance should be based on best practises and innovative multidisciplinary approaches for self –evaluating the effectiveness.

- Competent EU bodies and Data Protection Authorities should develop practical guidance documents that will be able to support and assist different types of data controllers.
- European research community and competent EU bodies should shift their focus on promoting EU policy implementation through innovative solutions and development guidelines

Demonstrating Compliance

Certification, marks and seals have served for years as useful indicators of adherence to pre-defined principles and characteristics. GDPR, under article 42, recognizes them as acceptable mechanisms assessing the level of data protection and demonstrating compliance.

- The European Commission should liaise with Data Protection Authorities and competent EU bodies and define the scheme and the operation of European data protection certification mechanisms, seals and marks.

Communication and Awareness Raising

With less than two years before GDPR provisions come into force, EU organizations are only starting to consider the changes they should undertake and broaden the perspective of their existing information security and business strategy.

- The European Commission, competent EU bodies and Data Protection Authorities should draw up and implement a strategy on communicating both the principles and transition compliance steps to GDPR provisions.

1. Introduction

1.1 Background

Small and Medium Enterprises (SMEs) are currently dominating the international business landscape[6] and constitute the backbone of the EU economy, promoting competiveness and investments of the Digital Single Market (DSM)[7,8]. In order to meet their objectives, SMEs are increasingly depending on Information Technology (IT) networks, systems and applications, while many have an online presence, offering digital services to their customers. They do so by establishing their own IT infrastructure and/or by relying on third party services and technologies, such as those of cloud computing services and Internet of Things (IoT) applications.

The high volume of SMEs subsequently reflects on the high volume of data that are processed by them, much of which is *personal data*. Personal data is defined under the EU General Data Protection Regulation (GDPR)[9] as 'any information relating to an identified or identifiable natural person (data subject)'. When processing personal data, SMEs have certain legal obligations arising from GDPR[10]. In particular, SMEs will very often take the role of the *data controller*[11], e.g. when processing personal data of customers or staff. Sometimes they may also take the role of *data processor*[12], e.g. when providing services to customers on behalf of another company. The criticality of the personal data processing performed by an SME may vary. For example, while a retail shop will only process personal data related to purchases of goods, a medical diagnostic centre will engage in the processing of health data of its clients and a dating site will maintain detailed personal profiles of its users.

One of the core obligations for data controllers and processors in GDPR is that of the *security of personal data*. In particular, according to GDPR security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk)[13]. Taking into account the increasing use of digital and/or online data processing systems, often based on cloud services and smart IoT

---

[6] As estimates suggest, more than 95% of enterprises across the world today are SMEs, see: http://www.edinburgh-group.org/media/2776/edinburgh_group_research_-_growing_the_global_economy_through_smes.pdf
[7] https://ec.europa.eu/growth/smes_en
[8] https://ec.europa.eu/growth/single-market/digital/
[9] 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 (General Data Protection Regulation), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[10] GDPR will be directly and commonly applicable to all Member States as of May 2018, repealing the current Data Protection Directive 95/46/EC. In the context of this document we refer to GDPR (and not the Directive) as the main legal framework for the protection of personal data in EU.
[11] Data controller is defined as: '*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*' (GDPR art. 4(7)).
[12] Data processor is defined as:' *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*' (GDPR art. 4(8)).
[13] This follows the overall principle of accountability that is enshrined in GDPR, establishing that the data controller shall be responsible for and able to demonstrate compliance with GDPR (GDPR art. 5(2)).

devices, security risks for personal data are associated today to a great extend to the security risks of the underlying IT networks and system components.

Over the last decade several security risk assessment methodologies and frameworks have been proposed by different bodies, aiming at supporting organizations in evaluating security risks associated with their business operations[14]. More recently, a few specific privacy risk assessment frameworks have also been presented, focusing particularly on the evaluation of risks to personal data and adoption of relevant security measures[15],[16],[17]. While big companies have the possibility to respond to and appropriately implement these frameworks, SMEs do not always have the necessary expertise and resources to do so. Indeed, it is in many cases difficult for SMEs to comprehend the specificities of the risks associated with personal data processing, as well as to assess and manage these risks following a formal methodology[18]. This can put on harm's way the personal data processed by SMEs, hindering at the same time compliance of SMEs with the GDPR legal obligations.

On this basis, ENISA within its Work Programme 2016[19] decided to provide further guidance to SMEs on how to adopt security measures for the protection of personal data, following a risk-based approach.

1.2 Scope and objectives

The overall scope of the present study is to provide guidelines for SMEs, acting as data controllers or processors, on adopting security measures for the protection of personal data, thus supporting them in achieving compliance with GDPR. In particular, the objectives of the report are twofold:

- Present a simplified approach that can help SMEs understand the context of the personal data processing operation and subsequently assess the associated security risks.
- Propose possible organizational and technical security measures for the protection of personal data, which are appropriate to the risk presented.

It should be noted that, although all types of data processing systems are covered, the study is mainly focused on electronic personal data processing by SMEs, which is based on IT networks and systems, as well as new digital technologies.

1.3 Structure

The structure of the document is as follows:

- Chapter 2 provides an introduction to information security and risk management, examining the specificities for personal data processing and relevant limitations of SMEs.

---

[14] See an inventory of risk assessment methodologies and tools in: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory
[15] https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
[16] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[17] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf
[18] Information security and privacy standards for SMEs: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport
[19] https://www.enisa.europa.eu/publications/corporate/enisa-work-programme-2016

- Chapter 3 presents a simplified approach for the evaluation of security risks by SMEs, providing guidance on how to address different steps of a privacy risk assessment process.
- Chapter 4 classifies possible security measures under different levels of risks. Both technical and organizational security measures are considered.
- Chapter 5 draws a number of final observations and conclusions with regard to the implementation of the proposed approach by SMEs, as well as possible future steps.

The target audience of this study comprises SMEs across the EU from all business sectors, as well as national Data Protection Authorities (DPAs) which can use the proposed approach to support their relevant data protection audit frameworks and security recommendations.

2. Security and risk management in the area of personal data

After a brief introduction to information security and security risk management, in this Chapter we discuss the specific characteristics of the security of processing of personal data, as well as the requirements of a data protection oriented risk management process, paying particular attention to the special needs and limitations of SMEs.

2.1 Introduction to information security

Information security encompasses all the measures taken to defend the information processed within a system (e.g. electronic, physical) from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The most used model to guide the development and implementation of a framework for managing information security within an organisation is represented by the so called CIA triad: confidentiality, integrity and availability of information.

Figure 1: The CIA triad

Confidentiality is defined as the "*property that information is not made available or disclosed to unauthorized individuals, entities, or processes*"[20]. In practice, all the measures implemented to ensure confidentiality are designed to prevent the information from being accessed by unauthorized individuals, entities or processes, while ensuring that the authorized individuals, entities or processes have access to it. In most cases the information is categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to these categories.

Integrity is defined as the property of "*accuracy and completeness*"[20]. In that sense, integrity implies maintaining the consistency, accuracy, and trustworthiness of information, over its entire life cycle. Data must not be changed in transit and measures must be undertaken to ensure that data cannot be altered by unauthorized individuals, entities or processes. From a practical point of view, this means that data cannot be modified in an unauthorized or undetected manner.

Availability is defined as the property of "*information being accessible and usable when an authorized party demands it*"[20]. This means that the systems used to store and process information, as well as the information communication channels are all functioning correctly. In practice this is best ensured by uncompromised maintenance of the hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is software conflicts free.

In the area of information security, there are several standards and frameworks providing for different types of controls[21], all following the CIA triad. The most known and widely employed is the ISO/IEC 27000 family

[20] ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary : http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=66435.
[21] https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data

of standards, which provide a systematic structured approach for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within an organization[22]. It consists of inter-related standards which cover different aspects of the ISMS lifecycle and aim to support the organization on a) identifying information assets and their associated information security requirements, b) assess and treat information security risks, c) select and implement relevant controls to manage unacceptable risks and finally d) monitor, maintain and improve the effectiveness of controls associated with the organization's information.

When embedding security measures in an information processing system, it is crucial to ensure that the CIA triad is applied in a balanced manner. While all three elements are important, different aspects of the triad will take priority depending on the industry and organization. To this end, the implementation of security measures needs to follow a *security risk management process*, as discussed in the next paragraph.

2.2 Information security risk management: an overview

Information security risk management is the process of identifying, quantifying, and managing the information security risks that an organisation faces; it is a process aimed at obtaining an efficient balance between realizing opportunities for gains and minimizing vulnerabilities and losses. As an integral part of management practices and an essential element of good governance, security risk management needs to be recurrent seeking to support organisational improvement, performance and decision making. ENISA has conducted a lot of work in the field of risk management, including an inventory of relevant methods, tools and good practices[23].

A risk management process comprises four key phases, as follows[24]:

- **Risk assessment**: It can be understood as the generation of a snapshot of current risks. A risk is often expressed as a function of the likelihood that an adverse outcome (threat) occurs multiplied by the magnitude of the adverse outcome (impact) should it occur. The risk assessment starts with the identification of threats, followed by the determination of the relevant likelihood and the impact of each risk. To properly assess the risk, one must take into consideration equally both likelihood and impact.
- **Risk treatment**: Based on the results of the risk assessment, at this phase the organization selects and implements security measures to treat the risks. The measures can have different effects, such as: mitigation, transfer, avoidance or retention of risks. Multiple security measures of different types can (and should) be used to treat the risks.
- **Risk acceptance**: Even when the risks have been treated, residual risks will probably remain (e.g. due to the fact that some controls are not feasible). These risks will need to be accepted. This is a management decision that needs to follow the acceptance of the way risks have been treated.
- **Risk communication**: All involved stakeholders need to be informed about risks adopted controls, as well as accepted risks.

[22] http://www.iso.org/iso/catalogue_detail?csnumber=54534
[23] For more information, see: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management
[24] See detailed analysis in ENISA's information packages for SMEs on risk assessment and risk management methods, https://www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes

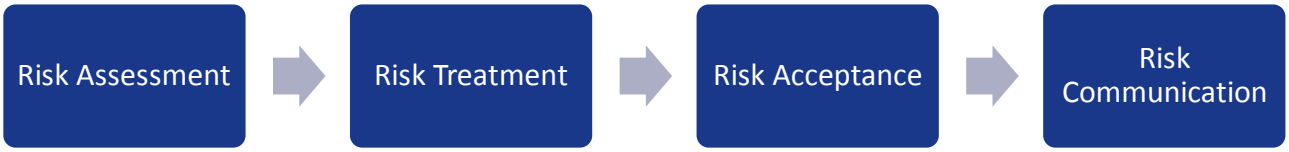

Figure 2: Security risk management phases

Risk management has greatly expanded since its inception and it is currently generally appreciated that risk cannot be reduced to zero and, thus, it is essential for an organization to be able to understand and assess it in order to prioritize resources.

2.3 Security for the processing of personal data

Personal data is also a type of information. Therefore, security of personal data follows in practice the general principles of information security and information security risk management, as these are presented in the previous paragraphs. Still, personal data have certain specificities that need to be considered when analysing security risks and adopting security measures. These specificities mainly arise from the underlying EU data protection legal framework (GDPR), as well the nature of personal data per se (as an information asset). In the next paragraphs we further explore these points, trying to define the particular characteristics of a security risk management framework for personal data.

2.3.1 Security obligations in GDPR

Although the security of personal data has always been a legal obligation for data controllers under the Data Protection Directive, GDPR reinforces the relevant provisions (both in substance and context), extending at the same time this responsibility directly also to data processors.

As a first point, it is important to note that security (in the sense of integrity and confidentiality) is established as one of the principles relating to personal data processing (Article 5 GDPR). This puts security at the core of data protection together with the rest of data protection principles, i.e. lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

Following this general principle, the security of personal data processing is mainly mandated in article 32 of GDPR, which states that:

'Having regard to the state of the art and the costs of implementation[25] and 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, the controller and the processor 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

[25] It is important to note that the reference to the "state of the art and cost of implementation" should not be interpreted as an excuse not to act, but rather as a call to all the stakeholders to simplify and reduce the costs, in order to spread the adoption of security measures. In that sense approaches towards simplification of the notion of risk and adoption of appropriate measures are key to the proper implementation of this article.

incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'

The article further stipulates that 'in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'. It also mentions that adherence to an approved code of conduct (Article 40 GDPR) or an approved certification mechanism (Article 41 GDPR) may be used as an element to demonstrate compliance with the requirements for the security of processing. Last, it states that the controller and processor 'shall take steps to ensure that any person acting under their authority and having access to personal data, shall not process them except on instructions from the controller, unless otherwise required by Union or member state law'.

Based on the aforementioned provisions, there are a number of important observations that should be made with regard to the security of personal data under GDPR:

- **Risk-based approach:** Technical and organisational measures for the protection of personal data should, according to GDPR, be appropriate to the risk presented. GDPR puts special emphasis on the notion of risk, establishing specific data protection parameters that need to be considered for its assessment, in particular the nature, scope, context and purposes of the processing. Moreover, it clearly relates the risk to the measures taken in order to preserve the rights and freedoms of individuals. This approach in fact introduces the impact of a potential personal data breach [26]to the data subjects as a major aspect of the risk assessment and should also be seen in relation to the requirement for a formal data protection impact assessment (under Article 35 GDPR). Having said that, it is also important to note that the notion of risk is central in general in GDPR as a threshold for the controller to implement different obligations, for example with regard to the notification of personal data breaches (Articles 33 and 34 GDPR), the conduction of data protection impact assessment the prior consultation with competent authorities (Article 36 GDPR).

- **An information management system for personal data:** The GDPR provision goes beyond the mere adoption of specific security measures, supporting the establishment of a thorough information management system for the protection of confidentiality, integrity, availability and resilience of personal data. This is important to outline as the text equally addresses all dimensions of information security, explicitly mandating for a process for testing, assessing and evaluating the effectiveness of the adopted measures.

- **Security for privacy:** Although GDPR does not provide a direct reference to privacy enhancing technologies (PETs)[27], it specifically addresses pseudonymisation and encryption as core protection measures for the security of personal data. This shows that security in GDPR is considered in the overall context of privacy and could include for example protection of identity through the use of pseudonyms or the use of encryption mechanisms for forcing secure data deletion after the end of the defined retention period. This point should also be linked to the provisions of GDPR for data protection by design and by default (Article 25), which put emphasis on the engineering of privacy requirements into IT systems and services, going beyond the 'traditional' understanding of security. It is interesting

[26] Personal breach is defined in GDPR as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.
[27] See more information on PETs and privacy by design in: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

to note that these provisions are also linked to the risk of personal data processing (which again works as a threshold for the adoption of relevant measures).

Finally, as shown also in the above points, it should be emphasized that security of processing is not an isolated obligation in GDPR, addressed under a particular article. On the contrary, it should be considered within the overall GDPR accountability framework for data protection, which is risk-based and impact-based and aims to fit into the overall operational context and practices of an organization. Under such framework, security measures can be seen on one hand as an obligation per se and on the other as a tool to implement other data protection obligations (e.g. those of data erasure and data subjects' rights), especially in online environments.

2.3.2 Security risk management for the processing of personal data

As previously discussed, the assessment and management of security risks is essential in information security, supporting the adoption of appropriate security measures. When applying this approach to personal data processing, however, one needs to consider the specificities of such processing, which require a different type of approach both in the assessment of the risks, as well as their treatment, acceptance and communication.

Following the analysis of paragraph 2.3.1, these specificities can be described as twofold:

- The notion of impact: In the 'typical' risk assessment process, the risks are estimated based on their potential impacts to the organization. In the case of personal data processing, however, the impacts are considered with regard to the freedoms and rights of individuals. This is a significant difference as it switches the analysis of impacts towards possible adverse effects that an individual may suffer, including for example identity theft or fraud, financial loss, physical or psychological harm, humiliation, damage to reputation or even threat to life. While performing such analysis the scale (e.g. number of affected individuals) may not be relevant: the impact is high even if it may bring severe adverse effects only to a single person. An additional challenge is that, in order to calculate the impact, possible secondary adverse effects to the rights and freedoms of individuals also need to be considered[28].

- The management of risks: Due to the privacy-specific notion of impact, the way that the identified risks are managed may also defer from the 'typical' risk assessment process. For example, even if the likelihood of a particular risk is low, a decision to accept the risk will not be the right choice when high impacts to particular individuals may occur (e.g. if it may cause them severe physical damage or threaten their life). In such a case, the data controller/processor would probably have to avoid the risk either by re-evaluating the overall processing operation or by utilizing specific privacy enhancing technologies (e.g. anonymization techniques). In the same way, the adoption of specific technical and organizational measures might be different between the 'typical' risk management process and the data protection risk management.

Therefore, in security risk management for personal data it is first of all important to define the overall context of the processing (e.g. types of personal data, purpose of processing, legitimate recipients, etc.), which will then support the definition of possible threats and risks based on the impact to individuals.

[28] See relevant examples in the Data Protection Working Party 29 Opinion 3/2014 on Personal Data Breach Notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

Appropriate technical and organisational controls will finally be adopted to manage the risks, taking into account the specificities relating to personal data.

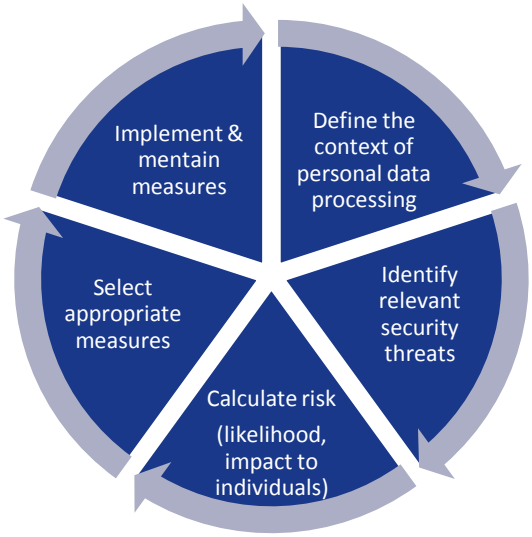

Figure 3: Security risk management for personal data

As shown in Figure 3, the process of security risk management for personal data does not in principle differ from the 'typical' security risk management models, but still it does need to incorporate the specificities of personal data processing as presented above.

2.4 Security of personal data in SMEs

According to the findings of a study regarding the global cost of data breaches in 2016[29], the average cost of data breaches has more than doubled between 2014 and 2015, while the average cost paid for each lost or stolen record containing sensitive and confidential information was slightly increased up to almost 150€. The main conclusions of this study suggest that overall the cost of a data breach has not fluctuated significantly over the years, which indicates that it is a permanent cost organizations need to be prepared to deal with and incorporate in their data protection strategies.

More specifically for the EU, half of the SMEs participating in a study regarding investing in the digital workplace[30] acknowledged data security as the major barrier, as it is difficult to bridge the ambitions of management with their limited budgets and perceived security. Indeed, most SMEs continue to trail behind on adopting information security since they only have a limited number of information security safeguards in place. Namely, the basic infrastructure and software components required for protecting their

[29] Ponemon Institute - 2016 Cost of Data Breach Study: Global Analysis http://www-03.ibm.com/security/data-breach/

[30] Are Europe's SMEs making the most of the Digital Workplace? A view into how small and medium businesses are embracing mobile tech https://dutchitchannel.nl/563254/rapport-are-europes-smes-making-the-most-of-the-digital-workplace.pdf

information assets (i.e. firewalls, anti-malware protection mechanisms etc.). Security and privacy controls are mainly implemented as part of the services or product packages SME acquire from their ICT providers and vendors. SMEs often have a small pool of IT resources and quite often the same resources are also responsible for information security and privacy tasks. In specific business areas (commerce, finance, etc.) they claim to have some security controls in place. However, the maturity and the rigour levels are very likely to vary depending on the type of security concerned as well as the interpretation of the specific area by each SME.

The scope and enforcement of GDPR brings with it challenges for SMEs through a single set of rules across the EU. SMEs are expected to manage their data flows and data processes to the same extent as bigger and better resourced organisations. Such obligations apply to cases where they not only act as data controllers but as data processors as well. For example, an SME offering data shredding and sanitizing services or cloud based storage is subject to these obligations, even if it is not a data collector. The GDPR provisions for a risk-based approach is horizontal as there are not exemptions or light weight approaches based on the organization size, availability of recourses and capabilities. Similar to larger organizations, SMEs have to identify the level of risk, depending on nature, scope, context of processing along to the types and volumes of data processed and proactively implement protective measures which correspond to the level of risk presented.

This contextual analysis of risks however, cannot be easily performed or even brought down to the level of an SME due to the broad differences among the aspects that have to be taken into account and the familiarization required with all GDPR provisions. Considering the specific characteristics of SMEs, such as limited resources, unavailability of qualified personnel and specific sectorial regulatory provisions, it is apparent that they could benefit from a more guided approach that will bridge the gap between the legal provisions and their understanding and perception of risk. Such guidance though should not be misinterpreted as a discount on the level of protection they are obliged to provide; on the contrary, it should be meant as an entry guide that will empower them to properly relate their processing activities to the legal provisions, understand the threats, determine the impact for the individual and identify the relevant security measures they should deploy.

Taking into account the aforementioned points, Chapters 3 and 4 present a simplified approach for calculating the risks for personal data processing and adopting security measures, targeting particularly the SMEs community.

3. Assessing security risks for personal data

The assessment of risks is the first step towards the adoption of appropriate security measures for the protection of personal data.

Following the analysis of Chapter 2, in this Chapter we present a simplified approach that can guide the SMEs through their specific data processing operation and help them evaluate the relevant security risks. As such, the proposed approach does not present a new risk assessment methodology but rather builds on existing work in the field[31,32,33] to provide guidance to SMEs.

It should be noted that the work is focused solely on security risk assessment and should not be confused with data protection impact assessment (DPIA - Article 35 GDPR). Indeed, while, the former is a critical part of the latter, a DPIA takes into account several other parameters that are related to the processing of personal data and go beyond security. Still, the proposed approach could also be useful in the context of a DPIA and/or could be extended in the future to also cover DPIA conduction.

The proposed approach is based on four steps, as follows:

- Definition of the processing operation and its context.
- Understanding and evaluation of impact.
- Definition of possible threats and evaluation of their likelihood (threat occurrence probability).
- Evaluation of risk (combining threat occurrence probability and impact).

The next paragraphs explain in more detail each of the steps.

The term 'organization' is used throughout this Chapter to refer to SMEs acting either as data controllers or data processors (under GDPR).

3.1 Step 1: Definition of the processing operation and its context

This step is the starting point of the risk assessment and is fundamental for the organization in order to define the boundaries of the data processing system (under assessment) and its relevant context. In doing so, the organization needs to consider the different phases of the data processing (collection, storage, use, transfer, disposal, etc.) and their subsequent parameters.

In the course of this exercise, the following questions need, as a minimum, to be asked and clearly understood (by the data controller/processor).

[31] CNIL – Managing Privacy Risks Methodology https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
[32] ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches https://www.enisa.europa.eu/publications/dbn-severity
[33] ENISA - Risk Management and Risk Assessment for SMEs https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/approaches-for-smes/infosec-smes/pilot-study

1. What is the personal data processing operation?

An important point to consider here is that it might be preferable to run different risk assessment processes for different data processing operations, even if these are managed through the same technical means (IT networks, systems, applications). This is especially important in case of processing operations that involve data of different nature and sensitivity and, thus, pose different levels of risks for the data subject.

Example: A company manages through its IT system the HR data (e.g. data on salaries, leaves, etc.) and data on purchase orders with external contractors. A different risk assessment process should in principle be followed for the two operations as in the first case the personal data involved are more critical (or even sensitive) and, thus, would probably result in a higher level of risk than the second case. This might also result in different types of security controls. If a single risk assessment exercise is conducted, the highest risk would at the end need to be considered (i.e. that of the HR system) for both processing operations.

2. What are the types of personal data processed?

Clearly linked to the previous question, the types of personal data can on one hand help define the processing operation, while on the other give an initial indication of the potential risk level.

Example: When special categories of data ('sensitive data') are involved, the risk is by default higher. Special categories of data include (Article 9 GDPR): data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. What is the purpose of the processing?

The purpose is directly linked to the data processing operation and can help the organization understand the limits of the processing (e.g. with regard to who gains access to the data and the way that access is provided). In the course of risk assessment, it might be necessary to distinguish data processing operations based on the purpose, even when the same types of data are involved.

Example: An SME processes name, postal and/or email address of its customers in the context of an online purchase service. The same types of data may be processed by the SME for sending marketing material (offers, newsletters) to customers. Still, the two processing operations, due to their distinct purposes, may present different types of risks that need to be more specifically addressed.

4. What are the means used for the processing of personal data?

The processing of personal data might take place in an automated or non-automated way or both, including particular IT networks, systems or applications. The SME might also rely partially or fully on the technical means of a data processor (e.g. cloud provider) for the provision of its service. It is important, thus, to clearly understand the means of the processing, paying particular attention to the fact that these may change in the different phases of the processing (collection, storage, use, transfer, disposal of personal data).

Example: A CRM (Customer Relationship Management) system can be used by an SME for the processing of customer personal data. An e-shop platform can be also used for on line sales and processing of customers' personal data. These systems might be hosted and maintained by the SME or the SME might be using relevant applications of a cloud provider (cloud as a service solutions).

5. Where does the processing of personal data take place?

The location of the personal data is also an important factor, especially when the services of data processors are used. It is important to note that when personal data are processed in a third (non-EU) country, additional protection mechanisms should be in place (Chapter V GDPR).

Example: In order to minimize costs and resources, an SME has outsourced part of its IT infrastructure and services (used for the processing of personal data) to a cloud provider with servers all over the world. In such a case, the SME should clearly specify with the cloud provider the location of the data and adopt the necessary controls (under GDPR).

6. Which are the categories of data subjects?

Clearly defining the data subjects (e.g. clients, customers, others) is important for the organization as part of the understanding of the data processing operation. In some cases, depending on the categories of data subjects, an indication of the potential risk level could already at this stage be obtained.

Example: Processing of personal data of children might require special attention due to the fact that children are often not made aware of the processing.

7. Which are the recipients of the data?

Defining the recipients of data helps in the understanding of authorised transfers or personal data, as well as the conditions of these transfers. Sometimes groups of recipients might be defined. Certain transfers may bear specific risks which already at this stage is good for the organization to acknowledge.

Example: An on-line dating site provides access to users' profiles to all registered users (as part of the provision of the service). It may also be requested to provide access to information related to subscription fees and payments to the state's financial audit services.

On top of the aforementioned questions, it is important that the organization is well aware of the legal basis that is used for the processing of the personal data, as well as all obligations arising from GDPR, including those for information of data subjects, exercise of data subjects' rights, etc. These points are not further discussed in this document but should be explicitly considered for achieving compliance with the data protection legislation.

3.2 Step 2: Understanding and evaluating impact

In this step the organization needs to evaluate the potential impact to the rights and freedoms of individuals that a security incident (related to the data processing system) might bring. The security incident may be associated to any type of breach of confidentiality, integrity or availability of personal data.

It should be noted that, due to the ad-hoc nature and variety of personal data processing, only a *qualitative approach* can be used, based on the overall understanding (by the organization) of its specific data processing operation. This approach is presented in the next paragraphs in more detail.

3.2.1 Levels of impact

Following previous work in the field[34,35], for the purpose of our proposed approach, we consider four levels of impact (Low, Medium, High & Very high), as shown in Table 1 below.

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 1: Levels of impact description

As indicated from the descriptions above, the level of impact is always co-related to the consequences that a personal data security breach might have to the individuals (whose data have been breached).

3.2.2 How to evaluate impact

As already mentioned, the evaluation of the impact can only be qualitative, taking into account the specificities of a particular data processing operation. In order to support the SMEs in this exercise, a number of parameters that need to be carefully considered (and co-related) are presented below[36]:

[34] CNIL – Managing Privacy Risks Methodology https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
[35] ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches https://www.enisa.europa.eu/publications/dbn-severity
[36] See also: ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches https://www.enisa.europa.eu/publications/dbn-severity

- **Type of personal data**: This parameter can, by nature, immediately increase or decrease the level of impact, based on the criticality of the data. For example, when the data include medical files or information on political beliefs (or any other special category of data under GDPR), the impact of a security breach can be severe for the individuals. Still, the assessment cannot only be based on the distinction of data between 'simple data' and special categories of data. Indeed, even personal data that do not fall under a special category can reveal very critical information about an individual (e.g. location, habits, financial information) and, thus, bring disastrous effects on him/her in case of a breach.

- **Criticality of the processing operation**: Following the aforementioned point, it is important to assess the overall criticality of the processing operation, beyond the particular types of data. Special consideration should be given to processing operations that are based on or may lead to the systematic tracking, monitoring or surveillance of individuals.

    - **Volume of the personal data processed**: This parameter relates to the quantity of personal data that is being processed for a single individual: the more the data, the more the potential adverse effects. Volume should be considered both in terms of time (e.g. same type of data over a certain period of time) and content (complementing data of the same type). For example, in case of a confidentiality breach of traffic data at a messaging service provider, the impact to an individual would be higher if these data cover the whole period of one year rather than if they are limited only to one week.

- **Special characteristics of the data controller/processor**: This parameter relates to the field of operation and the business activities of the organization, which may by nature be revealing additional information for a certain data set (thus, potentially affecting the level of impact). For example, the breach of confidentiality of a customers' list may be higher if this list comes from an online pharmacy than from a stationery shop.

- **Special characteristics of the data subjects**: The impact could also increase in case that the data subjects belong to a social group with particular needs (e.g. minors, public figures). For example, the processing of a list of telephone numbers becomes more critical if it concerns known members of the national parliament.

Examples:

Case 1 - A supermarket/restaurant processes the list of names and contact information of its customers, which are used to perform online purchases. No other personal data of customers are processed. In such case the impact could be considered as low since a potential security breach of these data may only bring minor inconveniences to the data subjects (e.g. unsolicited communication by advertisers), which can be easily overcome (e.g. registration to the Do-Not-Call register of their telephone service provider).

Case 2 - The supermarket/restaurant also processes the list of purchases and preferences of customers over the year. In such case, the impact could be considered medium if this list could lead to profiling of the data subjects' habits and preferences (e.g. based on what they buy and how often) and/or disclosure of further information (number of family members, special dietary needs, etc.). In case of breach of these data, the individuals might encounter significant inconveniences that they would probably still be able to recover with some difficulties (e.g. stress due to the disclosure of certain everyday habits).

Case 3 – A specialized electronic pharmacy selling products for diabetes patients processes the list of names and contact information of its customers. In such case, due to the special characteristics of this shop, which might even reveal sensitive data about certain individuals, the impact should be considered

as high. Indeed, in case of a confidentiality breach of these data, assumptions regarding the health status of the clients (diabetes) can be made, which can lead to significant consequences that are difficult to overcome (e.g. unwanted disclosure of this sensitive information to family members and friends).

Case 4 – An organisation supporting recovering drug-addicts to find employment processes names and CVs of these persons. In such case, the impact could be considered as very high, since a security (confidentiality) breach related to these data can lead to very serious consequences both for their physical and psychological situation, which can even be life-threatening.

Note that these examples should be considered only as indicative of the level of impact. The data controller/processor should always follow an in depth analysis, based on the specificities of its particular data processing operation.

On top of the parameters mentioned above, another important aspect that can be considered by the organization is the identifiability of the data subjects, i.e. how easy it is for a party who has access to the set of data to univocally relate them to a certain person. In order to consider identifiability, account should be taken both to possibilities of direct identification (e.g. on the basis of the data subject's name), as well as those of indirect identification (e.g. on the basis of an ID number or other identifier). Moreover, account should be taken to measures that might reduce the intelligibility of personal data (such as for example encryption), thus reducing the possibility of unauthorised disclosure of personal data[37].

Moreover, it is important to note that while evaluating the impact, possible secondary effects (to the rights and freedoms of individuals) should also be considered. For example, when the processing includes usernames/passwords to online profiles, account should be taken that individuals tend to re-use the same passwords over different online services (and, thus, a potential breach of these passwords might also lead to further personal data breaches).

Examples and information that can help the an organization (data controller/processor) understand and evaluate the impact can also be found in relevant work of the Data Protection Working Party 29[38] and the French Data Protection Authority[39].

3.2.3 Evaluation of impact

Based on the analysis of the previous section and the predefined impact levels (Table 1), in the context of our proposed approach, the organization is finally asked to evaluate the impact.

As shown in Table 2 below, the impact is assessed separately for the loss of confidentiality, integrity and availability (so as to again better support the controller/processor) in understanding the specificities of its

[37] See also Article 34 GDPR, where personal data breaches do not need to be communicated to affected individuals if data are encrypted.
[38] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
[39] CNIL – Managing Privacy Risks Methodology https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

personal data processing. It is important to consider all possible cases of unauthorised disclosure, alteration or destruction and evaluate the impact based on the worst-case scenario.

NO	QUESTION	EVALUATION
I.1.	**Please reflect on the impact that an unauthorized disclosure (loss of confidentiality) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.** ***Examples/scenarios of loss of confidentiality:*** • A paper file or laptop containing personal data is lost during transit. • Equipment has been disposed without destruction of the personal data. • Personal data are wrongly sent to a number of unauthorised recipients. • Some customers could access other customers' accounts in an online service. • Personal data are published on an internet message board or P2P site. • An CD-ROM with customer data has been stolen from premises. • A wrongly configured website makes publically accessible on internet data from internal users.	☐ Low ☐ Medium ☐ High ☐ Very high
I.2.	**Please reflect on the impact that an unauthorized alteration (loss of integrity) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.** ***Examples/scenarios of loss of integrity:*** • A record that is necessary for the provision of an online social service has been changed and the individual needs to ask for the service in an offline way. • A record that is important for the accuracy of an individual's file in an online medical service has been changed.	☐ Low ☐ Medium ☐ High ☐ Very high
I.3.	**Please reflect on the impact that an unauthorized destruction or loss (loss of availability) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.** ***Examples/scenarios of loss of availability:*** • A customer database is corrupted and some processing is required to bring the service online again. • A personnel file is lost and the individual needs to provide again some information to the company. • A file is lost/database corrupted and there is not back up of this information. • A critical service (e.g. online medical record) is down and cannot be immediately recovered.	☐ Low ☐ Medium ☐ High ☐ Very high

Table 2: Impact evaluation questions

After following the aforementioned assessment, three different levels of impact (for loss of confidentiality, integrity and availability) will be obtained. The highest of these levels should be considered as the final result of the evaluation of the impact, relating to the overall processing of personal data.

3.3 Step 3: Definition of possible threats and evaluation of their likelihood

In the context of this report, a threat is any circumstance or event which has the potential to adversely affect the security of personal data. At this step, the scope for the organization is to understand the threats related to the overall environment of the personal data processing (external or internal) and assess their likelihood (threat occurrence probability). Different levels and types of threats to the confidentiality, integrity and availability of personal data could be considered in this respect.

It should be noted that the context of the personal data processing (types of data, data subjects, etc.) is *not* considered as part of the threat occurrence probability, as it has been taken into account during the evaluation of the impact (step 2).

Examples of possible threats (to personal data)[40]:

- **An attacker injects code into the form of a website, aiming to gain access to the personal data stored in the system.**
- **An attacker performs a man-in-the-middle attack in order to intercept electronic communication.**
- **An employee steals personal data files from the internal system.**
- **A hospital's employee (maliciously or accidentally) changes a critical parameter in the medical file of a patient.**
- **Due to a power cut, the IT system of the customers' database is down.**
- **A USB flash drive with personal data files is lost in transit by a contractor.**

3.3.1 How to define the threats and their likelihood

In order to simplify this step for SMEs, we define a number of assessment questions that can help an organization (acting either as data controller or processor) in understanding the threats and calculating their occurrence probability. These questions in fact aim to support the assessment process by making the organization aware of the data processing environment (that is directly relevant to the threats). As such, they are related to four main dimensions of this environment, namely:

- **Network and technical resources (hardware and software):** Network connections may introduce threats both from external sources (e.g. external attackers aiming to remotely gain access to the system or bring the system down), as well as internal sources (e.g. interconnection with other IT systems within the same organization that have security flaws). Hardware and software resources may also introduce threats, e.g. due to poor maintenance and configuration, as well as due to bugs and backdoors related

[40] The CNIL methodology for privacy risk assessment (appendices) provides a detailed list of threats related to personal data processing, see in: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

to device and software development. Common threats associated to network and technical (hardware/software) resources include eavesdropping of communication channels, unauthorized access to databases, unavailability of provided services, failure of communication links, misuse/abnormal use of information systems, etc.

- **Processes/procedures related to the data processing operation:** In many cases security threats arise from the lack of appropriate internal processes and procedures, mandating specific rules and practices within the organization for the processing of personal data. Such threats include access to the data by unauthorized persons, (un)intentional corruption of data, unauthorised modification/destruction of data, accidental disposal or loss of data processing equipment, etc.
- **Different parties and people involved in the processing operation:** Security threats may also arise from those that perform the processing of personal data, i.e. the employees of the organization involved directly in the processing, as well as other parties conducting part of the processing (data processors). Relevant threats include potential malicious internal attacks (e.g. with the support of specific employees), accidental misuse of personal data due to human mistake, unauthorised disclosure of data by external contractors, etc.
- **Business sector and scale of the processing:** The business sector of an organization, as well as the scale (volume) of the data processed may also significantly affect the type and level of security threats. For example, if the type of personal data is considered a valuable asset and/or if the processing concerns the whole population of a country, attackers might be more interested in gaining access to these data.

These dimensions need to be considered having in mind the specific personal data processing operation and its characteristics, as these were defined in Step 1.

Table 3 below summarizes the proposed assessment questions, explaining the logic of each one of them and providing relevant examples towards assisting the organization to assess the level and likelihood of threats in each dimension.

A. NETWORK AND TECHNICAL RESOURCES		
1.	**Is any part of the processing of personal data performed through the internet?** *Examples:* • An e-marketplace offering the possibility of online purchase of goods • An e-news portal providing personalised information for registered users • A CRM system offered through a cloud as a service solution.	When the processing of personal data is performed fully or partially through the open Internet, possible threats from external online attackers increase (e.g. Denial of Service, SQL injection, Man-in-the-Middle attacks), especially when the service is available (and, thus, traceable/known) to all internet users.
2.	**Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?** *Examples:* • An insurance company allows remote access (through the internet) for managers to the clients' files. • A consulting company allows staff to access the internal system for managing leaves and missions through the internet. • A company provides remote access to the system to external contractors for IT maintenance and support.	When access to an internal data processing system is provided through the internet, the likelihood of external threats increases (e.g. due to external online attackers). At the same time the likelihood of (accidental or intentional) misuse of data by the users also increases (e.g. accidental disclosure of personal data when working in public spaces). Special attention should be given to cases where remote

		management/administration of the IT system is allowed.
3.	**Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service?** *Examples:* • An e-bookshop is connected to an online payment system (to support electronic purchases). • A small clinic finance IT system is connected to the IT system of national insurance scheme (to validate insurance status of the patients). • A CRM system interconnected with the IT system processing orders and systems supporting payments and invoice issuing.	Connection to external IT systems may introduce additional threats due to the threats (and potential security flaws) that are inherent to those systems. The same applies also to internal systems, taking into account that, if not appropriately configured, such connections may allow access (to the personal data) to more persons within the organization (which are not in principle authorized for such access).
4.	**Can unauthorized individuals easily access the data processing environment?** *Examples:* • An SME does not have a dedicated computer room for administering the IT system used for the processing of personal data. • An SME has outsourced the storage of its data to a company offering remote data storage. It is not clear what security measures have been applied by the company to safeguard the premises of the data centre.	Although focus has been put on electronic systems and services, the physical environment (relevant to these systems and services) is an important aspect that, if not adequately safeguarded, can seriously compromise security (e.g. by allowing unauthorized parties to gain physical access to the IT equipment and network components or failing to provide protection of the computer room in the event of a physical disaster).
5.	**Is the personal data processing system designed, implemented or maintained without following relevant documented best practices?** *Examples (of best practices in the field):* • The different network and system components are based on standard IT technologies and protocols (contrary to ad-hoc solutions). • Hardware and software is obtained by trusted providers and following formal contractual procedures. • A proper maintenance plan is in place, including regular maintenance of network and system devices and applications.	Poorly designed, implemented and/or maintained hardware and software components can pose serious risks to information security. To this end, best practices accumulate the experience of prior events and can be regarded as practical guidelines of how to avoid exposure and achieve certain levels of resilience.
B. PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA		
6.	**Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?** *Examples:* • Assistants in the financial department cannot only enter information, but also modify and delete it, same as managers. • The nurses in a medical clinic can modify the patient's medical file, although only doctors should be able to do so.	When roles and responsibilities are not clearly defined, access (and further processing) of personal data may be uncontrolled, resulting to unauthorized use of resources and compromising the overall security of the system.
7.	**Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined?** *Examples:* • It is not clear if employees can use their professional email address for personal communications.	When acceptable use of resources is not clearly mandated, security threats might arise due to misunderstanding or intentional misuse of the system. The clear definition of policies for network, system

	• There is no policy in place mandating the level of bandwidth usage that employees are allowed to on a daily basis.	and physical resources can reduce potential risks.
8.	**Are the employees allowed to bring and use their own devices to connect to the personal data processing system?** *Examples:* • Employees can connect to the company's network with their tablets or other smart devices. • Employees are allowed to process data using specific applications installed in their personal tables/smart devices.	Employees using their personal devices within the organization could increase the risk of data leakage or unauthorized access to the information system. Moreover, as devices are not centrally controlled, they may introduce additional bugs or viruses into the system.
9.	**Are the employees allowed to transfer, store or otherwise process personal data outside the premises of the organization?** *Examples:* • A travel agency allows employees to use their professional laptops outside the premises of the organization in order to process clients' data. • A delivery company allows employees to use dedicated tablets while making the delivery to validate details of the recipient.	Processing of personal data outside the premises of the organization can offer a lot of flexibility, but at the same time introduces additional risks, both related to the transmission of information through possibly insecure network channels (e.g. open Wi-Fi networks), as well as unauthorised use of this information.
10.	**Can personal data processing activities be performed without log files being created?** *Examples:* • There is no list of persons accessing the computer room of a company on daily basis. • Access to the medical files of patients in a clinic is not registered. • There is no policy in place mandating how the logs are monitored and what actions should be taken in case of repeated abuse of the system.	The lack of appropriate logging and monitoring mechanisms can increase intentional or accidental abuse of processes/procedures and resources, resulting to the subsequent abuse of personal data.
C. PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA		
11.	**Is the processing of personal data performed by an undefined number of employees?** *Examples:* • The HR ticketing system of a company can be viewed by all staff members. • Medical records of patients can be processed by secretaries although only treating medical staff should have access.	When access (and further processing) of personal data is open to a large number of employees, the possibilities of abuse due to human factor increase. Clearly defining who really needs to access the data and limiting access only to those persons can contribute to the security of personal data.
12.	**Is any part of the data processing operation performed by a contractor/third party (data processor)?** *Examples:* • The IT system of a private school is hosted at an external data centre. • The client files of an insurance company are being processed by external associates of the company • A specialised company is contracted for the destruction of patient files in a medical clinic. • A company uses a Cloud as a Service solution to manage internal resources.	When the processing is performed by external contractors, the organization may lose partially the control over these data. Moreover, additional security threats may be introduced due to the threats that are inherent to these contractors. It is important for the organization to select contractors that can offer a high level of security and to clearly define what part of the processing is assigned to them, maintaining as much as possible a high level of control.

13.	**Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?** *Examples:* • Employees are not clearly informed that they are processing confidential information which may not be disclosed to unauthorised parties. • External associates of a company are not given clear instructions regarding the required level of security of personal data processed by them.	When employees are not clearly informed about their obligations, threats from accidental misuse (e.g. disclosure or destruction) of data many significantly increase.
14.	**Is the personnel involved in the processing of personal data unfamiliar with security matters?** *Examples:* • Not all persons involved in data processing are informed about possible security threats and proper use of resources. • The staff handling the telephone centre of a company has not been informed about possible phishing and targeted attacks.	When employees are not aware of the need of applying security measures, they can accidentally pose further threats to the system. Training can greatly contribute in making employees aware both of their data protection obligations, as well as the application of specific security measures.
15.	**Do the persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?** *Examples:* • HR data of employees are not kept in locked file cabinets. • Copies of received invoices with credit card and bank account details are not being destroyed with paper shredders, after being processed.	Many personal data breaches occur due to the lack of physical protection measures, such as locks and secure destruction systems. Paper based files are usually part of the input or the output of an information system, can contain personal data and should also be protected from unauthorized disclosure and re-use.
D. BUSINESS SECTOR AND SCALE OF PROCESSING		
16.	**Do you consider your business sector as being prone to cyberattacks?** *Examples:* • A number of companies (of the same sector) were attacked during the last year. • Publicity has been given to possible security threats and vulnerabilities of the particular business sector (e.g. as a result of a study).	When security attacks have already taken place in a specific business sector, there is an indication that the organization would probably need to take additional measures to avoid a similar event.
17.	**Has your organization suffered any cyberattack or other type of security breach over the last two years?** *Examples:* • The IT department has discovered an increased number of unsuccessful attempts from external systems to gain unauthorised access to the database. • Locks in the central data centre have been violated.	If the organization has already been attacked or there are indications that this might have been the case, additional measures need to be taken to prevent similar events in the future.
18.	**Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?** *Examples:* • Users of the online service of an e-shop have notified that they could accidentally access accounts of other users.	Security bugs/wholes can be exploited to perform attacks (cyber or physical) to systems and services. Information regarding such cases should be considerably considered.

	• Auditors have found that the password policy utilised by an online service is weak.	
19.	**Does your processing operation concern a large volume of individuals and/or personal data?** *Examples:* • An online patient record application of a hospital which stores data of chronic disease patients all over the country. • An online dating site which stores profiles of hundreds of users.	The type and volume of personal data (scale) can make the processing operation attractive to attackers (due to the inherent value of these data).
20.	**Are there any security best practices specific to your business sector that have not been adequately followed?** *Examples (of possible sector specific practices):* • A company subject to specific security measures for medical devices, financial services or telecommunication services.	Sector specific security measures are usually adjusted to the needs (and risks) of the particular sector. Lack of compliance with relevant best practices might be an indicator of poor security management.

Table 3: Questions for assessing the threats and their likelihood in a personal data processing environment

After answering the questions presented in Table 3, the organization should be in a position of better understanding the threats associated with its data processing environment, as well as the likelihood of these threats. In each one of them, a positive reply (YES) indicates a high threat probability while a negative answer (NO), a lower threat probability. Based on this understanding, the assessment of the threat occurrence probability can follow.

It should be noted that, even though the aforementioned questions (and overall approach) aim to cover a broad spectrum of both external and internal security threats, they cannot be considered as exhaustive but rather perceived as indicative of the practical evaluation of threats (and their occurrence). In that sense, additional factors, and therefore assessment areas, might need to be taken into account by the organization, following the specificities of its personal data processing environment.

3.3.2 Evaluation of threat occurrence probability

As in the case of the evaluation of impact, the assessment of threat occurrence probability can only be qualitative, as it is very much related to the specific personal data processing environment. In the context of our approach, we define three levels of threat occurrence probability, namely:

- Low: the threat is unlikely to materialize.
- Medium: it is possible that the threat materializes.
- High: the threat is likely to materialize.

Following the above levels, the organization is asked to assess the likelihood of threats for each of the four different areas defined under Table 3, i.e. network and technical resources, processes/procedures related to the processing of personal data, parties/people involved in the processing of personal data, business sector and scale of processing (Table 4). If all replies, in an assessment area, are positive, then the organization should consider the threat probability for this area as high, while if all are negative, then the threat probability should be considered as low. For cases with two to three positive answers organization should assign the threat probability to medium. As discussed earlier, the questions cannot be considered as

exhaustive but only as indicative and consequently so is the correlation of positive/negative answers to threat occurrence probability levels.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐ Low	1
	☐ Medium	2
	☐ High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	☐ Low	1
	☐ Medium	2
	☐ High	3

Table 4: Assessing threat occurrence probability per area

The final threat occurrence probability is calculated after summing up the four different scores obtained under Table 4 and associating the result to the scales of Table 5 below.

THREAT OCCURRENCE PROBABILITY SCALE	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 -12	High

Table 5: Evaluation of threat occurrence

3.4 Step 4: Evaluation of risk

After evaluating the impact of the personal data processing operation and the relevant threat occurrence probability, the final evaluation of risk is possible, as shown in Figure 4 and Table 6 below.

Figure 4: Final risk evaluation

The population of the risk matrix below with risk levels was performed on the assumption of the worst-case scenario (highest possible impact on the individual). Consequently, the impact level was weighted more than the threat occurrence probability and only two low risk and three medium risk levels have been identified. High and Very High Impact levels have all been assigned to high risk levels and have been merged.

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

Legend

Low Risk *Medium Risk* *High Risk*

Table 6: Evaluation of risk

Independently of the final result of this exercise, the organization should feel free to adjust the obtained risk level, taking into account specific characteristics of the data processing operation (that have been missed during the assessment process) and providing adequate justification for this adjustment.

4. Security Measures

Following the evaluation of the risk level, the organization can proceed with the selection of appropriate security measures for the protection of personal data. In this Chapter, two main categories of measures are discussed: organizational and technical ones. These broad categories have been further divided to subcategories with a short description, explaining how each subcategory relates to specific provisions of GDPR.

Under each subcategory measures are presented per risk level, following the same colouring scheme used in Chapter 3 (low: green, medium: yellow, high: red). In order to achieve scalability, it is assumed that all measures described under the low level (green) are applicable to all levels. Similarly, measures presented under the medium level (yellow) are applicable also to high level of risk. Measures presented under the high level (red) are not applicable to any other level of risk.

It should be noted that the match of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive[41] or the NIS Directive[42]. In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013[43] security controls is also included.

4.1 Organizational security measures

4.1.1 Security management

4.1.1.1 Security policy and procedures for the protection of personal data

The security policy is a high level document that sets the basic principles for the security and protection of personal data in an organization. It, thus, forms the basis for the implementation of all specific technical and organizational measures, according to art. 32 GDPR, as also complemented by art. 24 GDPR (implementation of data protection policies).

Based on the security policy, the specific technical and organizational measures are described in a set of more detailed policies/procedures (e.g. on access control, device management, resource management, etc.).

The security policy shows the overall commitment of the organization's management towards security and data protection. It can be based on or form part of the organization's general IT security policy; in any case, it should explicitly address also the protection of personal data.

[41] Directive 2002/58/EC on privacy and electronic communications: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058

[42] Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1481193515962&uri=CELEX:32016L1148

[43] ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=54534

A.1	The organization should define its policy with regards to personal data processing as part of its information security policy.	
A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	
A.3	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	
A.4	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	
A.5	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	
A.6	The security policy should be reviewed and revised, if necessary, on a semester basis.	
	Related to ISO 27001:2013 - A.5 Security policy	

4.1.1.2 Roles and responsibilities

According to art. 32 (4) GDPR, '*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*'.

Therefore, as a first and basic control for the security of personal data, all organization's posts with access to personal data should have clearly defined and documented responsibilities, roles and a need to know basis (which are regularly reviewed and refined).

A role of particular importance is that of the Security Officer, who is responsible for the monitoring of the proper implementation of the security policy. Another important role is that of the Data Protection Officer (DPO), who is monitoring compliance with GDPR and, thus, clearly also needs to collaborate with the Security Officer in adequately implementing security measures. It should be noted that under GDPR (art. 37) the designation of a DPO is mandatory for certain types of data processing operations (large scale monitoring activities, processing of special categories of data, etc.).

B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	
B.2	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	

B.3	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.	
B.4	The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.	
B.5	Conflicting duties and areas of responsibility, for examples the roles of security officer, security auditor, and DPO, should considered to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.	
	Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities	

4.1.1.3 Access control policy

Following the definition of roles and responsibilities, it is essential to determine an access control policy to the systems used for the processing of personal data. This should be based on the 'need to know' principle, i.e. each role/user should only have the level of access to personal data that is strictly necessary for the performance of its relevant tasks. This is a central concept also in GDPR and is closely related to the principle of data minimization (art. 5(c) GDPR).

The access control policy will be implemented with subsequent technical measures (see also 4.2.1 in this document).

C.1	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.	
C.2	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.	
C.3	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.	
C.4	Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.	
	Related to ISO 27001:2013 - A.9.1.1 Access control policy	

4.1.1.4 Resource/asset management

The proper management of hardware, software and network resources is essential for the security of personal data, as it allows control of the means of the processing (and, thus, control of the subsequent organisational and technical measures). Resource management as a minimum includes the registration of IT resources and network topology (which are used for the processing of personal data).

D.1	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).	
D.2	IT resources should be reviewed and updated on regular basis.	
D.3	Roles having access to certain resources should be defined and documented.	
D.4	IT resources should be reviewed and updated on annual basis.	
	Related to ISO 27001:2013 - A.8 Asset management	

4.1.1.5 Change management

Change management aims at synchronizing and controlling all changes performed in the IT system used for the processing of personal data. It is an important security measure, as an unsuccessful change attempt could lead to unauthorised disclosure, modification or destruction of data.

E.1	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.	
E.2	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.	
E.3	A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.	
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities	

4.1.1.6 Data processors

According to art. 28 GDPR, '*the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*'. The same article states that the processing by the processor should necessarily be governed by contract or other legal act, setting also the minimum clauses that this should include and particularly referring to the security of personal data under article 32 GDPR.

F.1[44]	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.	
F.2[44]	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.	
F.3[44]	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.	
F.4	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.	
F.5	The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.	
	Related to ISO 27001:2013 - A.15 Supplier relationships	

4.1.2 Incident response and business continuity

4.1.2.1 Incidents handling / Personal data breaches

In the event of a data security breach, the organization should asses if this leads to an "*accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (art. 4(12) GDPR). Data controllers should make sure that they meet their obligations under articles 33 and 34 GDPR regarding notification of a personal data breach to the supervisory authority and to the data subjects. Data processors should also make sure that they meet their obligation under article 33 GDPR for immediate notification of the data controller. In any case, both data controllers and processors should have appropriate procedures in place, not only for the notification of personal data breaches, but also for the overall handling and management of such events.

G.1	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.	
G.2	Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.	
G.3	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.	

[44] These measures are mandated as obligations by Article 28 GDPR.

G.4	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.	
	Related to ISO 27001:2013 - A.16 Information security incident management	

4.1.2.2 Business continuity

A business continuity plan (BCP) is essential for determining the processes and technical measures that the organization should follow in case of an incident/personal data breach. As such it complements the security policy of the organization, as well as its incidence response plan. This measure is clearly related to art. 32 GDPR, which mandates the ability (for the controller/processor) '*to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*".

H.1	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).	
H.2	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.	
H.3	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.	
H.4	An alternative facility should be considered, depending on the organization and the acceptable downtime of the IT system.	
	Related to ISO 27001:2013 - A. 17 Information security aspects of business continuity management	

4.1.3 Human resources

4.1.3.1 Confidentiality of personnel

In order to ensure confidentiality of personal data under art. 32 GDPR, the organization should ensure that its employees also provide sufficient confidentiality guarantees, both in terms of technical expertise and personal integrity. Moreover, according to art. 32 (4) GDPR, '*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*'. To this end, specific measures should be in place to ensure that the personnel involved in the processing of personal data is properly informed about its duty to confidentiality, as well as to guarantee that this duty is sufficiently stipulated in the organization's human resources policies.

I.1	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.	
I.2	Prior to up taking their duties employees should be asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.	
I.3	Employees involved in high risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).	
	Related to ISO 27001:2013 - A.7 Human resource security	

4.1.3.2 Training

Personnel training in data protection and security procedures (e.g. use of passwords and access to specific data processing systems) is important for the right implementation of the organizational and technical security measures. Information on specific data protection legal obligations is also central, especially for key personnel involved in high risk processing of personal data.

J.1	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	
J.2	The organization should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.	
J.3	A training plan with defined goals and objectives should be prepared and executed on an annual basis.	
	Related to ISO 27001:2013 - A.7.2.2 Information security awareness, education and training	

4.2 Technical security measures

4.2.1 Access control and authentication

Access control and authentication are basic security measures for the protection against unauthorised access to the IT system used for the processing of personal data. They implement the access control policy of the organization (see Section 4.1.1.3) by technically enforcing it into specific components and applications.

K.1	An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.	
K.2	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.	
K.3	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.	
K.4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.	
K.5	A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.	
K.6	User passwords must be stored in a "hashed" form.	
K.7	Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.	
K.8	Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.	
	Related to ISO 27001:2013 - A.9 Access control	

4.2.2 Logging and monitoring

The use of log files is an essential security measure that enables identification and tracking of user actions (with regard to the processing of personal data), thus supporting accountability in case of an unauthorised disclosure, modification or destruction of personal data. Monitoring of log files is important for identifying potential internal or external attempts for system violation.

L.1	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).	
L.2	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source	
L.3	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.	
L.4	There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.	

L.5	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.	
	Related to ISO 27001:2013 - A.12.4 Logging and monitoring	

4.2.3 Security of data at rest

Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Therefore, this category of measures is mainly related to the processing of personal data in databases or other relevant systems (including cloud storage). It also relates to the processing of personal data by employees with the use of specific workstations or other devices. GDPR recognizes the ability of pseudonymization to help protect the rights of individuals while also enabling data utility. Under article 32, one of the measures mentioned is the "pseudonymization and encryption of personal data".

4.2.3.1 Server/Database security

Servers and databases consist the backbone of the information system processing personal data. They must be security hardened to ensure a secure operating environment.

M.1	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	
M.2	Database and applications servers should only process the personal data that are actually needeeds to process in order to achieve its processing purposes.	
M.3	Encryption solutions should be considered on specific files or records through software or hardware implementation.	
M.4	Encrypting storage drives should be considered	
M.5	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information	
M.6	Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.	
	Related to ISO 27001:2013 - A. 12 Operations security	

4.2.3.2 Workstation security

This measure is mainly related to the security configuration of users' workstations or other devices. It is important for enforcing specific security policies and restricting users from performing certain actions that

could compromise the security of the IT system (e.g. deactivating of antivirus programs or installation of unauthorised software).

N.1	Users should not be able to deactivate or bypass security settings.	
N.2	Anti-virus applications and detection signatures should be configured on a weekly basis.	
N.3	Users should not have privileges to install or deactivate unauthorized software applications.	
N.4	The system should have session time-outs when the user has not been active for a certain time period.	
N.5	Critical security updates released by the operating system developer should be installed regularly.	
N.6	Anti-virus applications and detection signatures should be configured on a daily basis.	
N.7	It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).	
N.8	Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorised processing, copying and transfer of personal data on store.	
N.9	Full disk software encryption should be enabled on the workstation operating system drives	
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems	

4.2.4 Network/Communication security

Network security is important for the protection of personal data, both with regard to external connections (e.g. to the Internet), as well interconnection with other systems (external or internal) of the organization.

O.1	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	
O.2	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.	

O.3	Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.	
O.4	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.	
O.5	The network of the information system should be segregated from the other networks of the data controller.	
O.6	Access to the IT system should be performed only by pre-authorized devices and terminal using techniques such as MAC filtering or Network Access Control (NAC)	
	Related to ISO 27001:2013 - A.13 Communications Security	

4.2.5 Back-ups

A back up system is an essential means of recovering from the loss or destruction of data. While some system should be in place, the frequency and nature of back up will depend, amongst other factors, on the type of organisation and the nature of data being processed. Under GDPR article 32 the aspect the “ability to restore the availability and access to personal data” in part of the data security obligations for the data controller or data processor.

P.1	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	
P.2	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	
P.3	Execution of backups should be monitored to ensure completeness.	
P.4	Full backups should be carried out regularly.	
P.5	Backup media should be regularly tested to ensure that they can be relied upon for emergency use.	
P.6	Scheduled incremental backups should be carried out at least on a daily basis.	
P.7	Copies of the backup should be securely stored in different locations.	

P.8	In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the data controller.	
P.9	Copies of backups should be encrypted and securely stored offline as well.	
	Related to ISO 27001:2013 - A.12.3 Back-Up	

4.2.6 Mobile/Portable devices

Mobile/Portable devices can extent the level of services offered by the data controller but increase exposure to theft and accidental loss. In the case of mobile devices, such as smartphones or tablets, users might also apply them for personal use and special care must be taken to ensure that business data is not compromised.

Q.1	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	
Q.2	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	
Q.3	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	
Q.4	Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.	
Q.5	The organization should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.	
Q.6	Mobile devices should support separation of private and business use of the device through secure software containers.	
Q.7	Mobile devices should be physically protected against theft when not in use.	
Q.8	Two factor authentication should be considered for accessing mobile devices	
Q.9	Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.	
	Related to ISO 27001:2013 - A. 6.2 Mobile devices and teleworking	

4.2.7 Application lifecycle security

During all phases of application development lifecycle, the organization must ensure that data protection compliance, including personal data security, is taken into consideration. In article 25 GDPR introduces the principles of data protection by design and by default which require data controllers to design and implement processing activities with data protection in mind while applying the strictest privacy settings.

R.1	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	
R.2	Specific security requirements should be defined during the early stages of the development lifecycle.	
R.3	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	
R.4	Secure coding standards and practises should be followed.	
R.5	During the development, testing and validation against the implementation of the initial security requirements should be performed.	
R.6	Vulnerability assessment, application and infrastructure penetration testing should be performed by a trusted third party prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved.	
R.7	Periodic penetration testing should be carried out.	
R.8	Information about technical vulnerabilities of information systems being used should be obtained.	
R.9	Software patches should be tested and evaluated before they are installed in an operational environment.	
	Related to ISO 27001:2013 - A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes	

4.2.8 Data deletion/disposal

The purpose of disposal/deletion is to irreversibly delete or destroy the personal data so that it cannot be recovered. The method(s) used must, therefore, match with the type of storage technology, including paper based copies. When disposing obsolete or redundant equipment, the data controller must ensure that all data previously stored on the devices has been removed prior to disposal. According to article 6 GDPR personal data should not be retained for longer than necessary in relation to the purposes for which they were collected, or for which they are further processed. In some cases, data subjects are also entitled to request deletion prior to the end of the maximum retention period.

S.1	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	
S.2	Shredding of paper and portable media used to store personal data shall be carried out.	
S.3	Multiple passes of software-based overwriting should be performed on all media before being disposed.	
S.4	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate.	
S.5	Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.	
S.6	If a third party, therefor data processor, is being used for destruction of media or paper based files, it should be considered that the process takes place at the premises of the data controller (and avoid off-site transfer of personal data.	
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment	

4.2.9 Physical security

Physical security is equally important to the technology-oriented security measures as physical access to the information system can be the foundation for the overall security strategy.

T.1	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	
T.2	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate.	
T.3	Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored	
T.4	Intruder detection systems should be installed in all security zones.	
T.5	Physical barriers should, where applicable, be built to prevent unauthorized physical access.	

T.6	Vacant secure areas should be physically locked and periodically reviewed	
T.7	An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room	
T.8	External party support service personnel should be granted restricted access to secure areas.	
	Related to ISO 27001:2013 - A.11 – Physical and environmental security	

5. Conclusions

The Digital Single Market Strategy is expected to maximise the growth potential of the European Digital Economy and European SMEs, which comprise a big part of it. However, as nowadays products and services are created and delivered through a value chain based on IT technologies and information sharing, organizations must guarantee an adequate level of protection for the personal data they collect, process and store. Although security of personal data has always been a legal obligation for data controllers, the imminent General Data Protection Regulation reinforces the relevant provisions (both in substance and context), extending at the same time this responsibility directly also to data processors while embracing a risk based approach. This contextual analysis of risks however, cannot be easily performed or even brought down to the level of an SME due to the broad differences among the aspects that have to be taken into account and the familiarization required with all GDPR provisions.

Considering the specific characteristics of SMEs, such as limited recourses, unavailability of qualified personnel and specific sectorial regulatory provisions, ENISA aimed to support them, through practical guidelines, on how to calculate the risks for personal data processing and adopt appropriate security measures. The approach undertaken should not be considered as exhaustive but rather as an attempt to bridge the gap between the legal provisions and SMEs understanding and perception of risk.

On top of the aforementioned work, a number of challenges were also identified at a broader EU level and respective conclusions were drawn for all involved stakeholders, as follows:

No *one-size-fits-all* approach

GDPR provision for a risk-based approach is horizontal as there are not exemptions or light weight approaches based on the organization size, availability of recourses and capabilities. Similar to larger organizations, SMEs have to identify the level of risk, depending on nature, scope, context of processing along to the types and volumes of data processed. However as personal data processing operations differ among data controllers, so will the overall risk based approach which extends beyond the data security provisions.

Guidance Needed

The GDPR provision goes beyond the mere adoption of specific security measures, supporting the establishment of a thorough information security management system for the protection of confidentiality, integrity, availability and resilience of personal data. In However SMEs are not fully acquaint to the perception of risk from the personal data perspective and they could benefit from a more guided approach that will bridge the gap between the legal provisions and their understanding and perception of risk. Such guidance should be based on best practises and innovative multidisciplinary approaches for self –evaluating the effectiveness.

Competent EU bodies and Data Protection Authorities should develop practical guidance documents that will be able to support and assist different types of data controllers.

European research community and competent EU bodies should shift their focus on promoting EU policy implementation through innovative solutions and development guidelines.

Demonstrating Compliance

Certification, marks and seals have served for years as useful indicators of adherence to pre-defined principles and characteristics. GDPR, under article 42, recognizes them as acceptable mechanisms assessing the level of data protection and demonstrating compliance. Emphasis is given to the specific needs of SME's, as on the one hand they are gradually relying more and more on third party technologies, products and services and on the other hand, GDPR compliance can also constitute a competitive advantage. Building on the experience of European Privacy Seal[45] and the ongoing discussions on a European ICT security certification framework for products and services, as described in COM(2016) 410[46], a harmonised, scalable and transparent data protection certification mechanism with relevant standards should be established.

The European Commission should liaise with Data Protection Authorities and competent EU bodies and define the scheme and the operation of European data protection certification mechanisms, seals and marks.

Communication and Awareness Raising

With less than two years before GDPR provisions come into force, EU organizations are only starting to consider the changes they should undertake and broaden the perspective of their existing information security and business strategy. However, the extent of change required and how changes will affect the organization cannot be foreseen. Organizations should therefore be communicated the need for shifting approach along to the requirements and specific guidelines or recommendations.

The European Commission, competent EU bodies and Data Protection Authorities should and Competent EU bodies Data Protection Authorities and EU bodies should draw up and implement a strategy on communicating both the principles and transition compliance steps to GDPR provisions.

[45] www.european-privacy-seal.eu
[46] EC COM(2016) – 410 Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-05-16-090-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-209-7
DOI: 10.2824/867415