Reinforcing trust and security in the area of electronic communications and online services

Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing

DECEMBER 2018

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 EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists 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 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.

Contributors

Fabio Guasconi (Bl4ckswan), Georgia Panagopoulou (HDPA), Giuseppe D'Acquisto (Garante), Athena Bourka (ENISA), Prokopios Drogkaris (ENISA)

Editors

Prokopios Drogkaris (ENISA), Athena Bourka (ENISA)

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-284-4, DOI 10.2824/015812

Table of Contents

Executive Summary

The General Data Protection Regulation (GDPR)[1] has reinforced the provisions on security of personal data (both in substance and context) and also extended this responsibility directly to data processors. Beyond being a principle (namely a prerequisite) for the processing, security is one of the main elements of controllers' accountability. This means that compliance cannot be merely formal and based on the implementation of closed checklists, but linked to the "context" where the processing operation takes place and the actual risks. As such, it requires an engineered approach capable of striking a balance between security goals, costs and "state- of-the-art" solutions.

The notion of the state-of-the-art relates to the most recent stage of technological development, or otherwise the stage that incorporates the newest possible features and functionalities. The cost of implementation is clearly linked to the state-of-the-art, as technical solutions also need to be applicable in practice. In that sense, costs should be interpreted both in terms of budget, as well as in terms of human resources required for implementation of specific security measures. On this basis and as part of its continuous support on EU policy implementation, ENISA published in 2017 a set of guidelines for SMEs[2], acting as data controllers or processors, which aim at helping them assess security risks and accordingly adopt security measures for the protection of personal data. Those guidelines can also be of use in all cases where risk assessment is envisaged under the Regulation (e.g. Data Protection Impact Assessment, personal data breach notification, etc).

This study provides an overview of well-established security practices, for the purpose of sketching the notion of "state-of-the-art" in a number of categories of measures, as they are listed in ENISA's guidelines for SMEs on the security of personal data processing. In particular, a number of categories of security measures have been analysed, taking into consideration specific aspects that are relevant to the processing of personal data. Overall, the outcome of this report is to complement relevant ENISA studies in the greater area of security of personal data processing. To this end, the study provides for a general and simple description of key security measures without providing specific technical implementation details.

The target audience of the report is mainly SMEs, acting as data controllers and data processors that can use the guidance on well-established technical and organizational measures while pursuing compliance with the GDPR. Data Protection Authorities (DPAs) might also find this analysis of interest in the context of their own data protection audit frameworks and security recommendations. On top of the aforementioned work, a number of challenges were also identified at a broader EU level and respective recommendations were identified for all involved stakeholders, as follows:

- The research community should continue working on providing innovative technical solutions to the ever-increasing security threats in the areas of security measures and privacy enhancing technologies, with the support of competent EU bodies, in terms of policy guidance and funding mechanisms.
- European Commission, 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 on the selection of appropriate and adequate security measures.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

[2] ENISA - Guidelines for SMEs on the security of personal data processing https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

- The research community and competent EU or standardization bodies, in close collaboration with regulators (e.g. Data Protection Authorities), should propose and put forward methodologies and practical ways (e.g. certification) to support data controllers/processors on assessing their level of compliance and exposure to risk.

1. Introduction

1.1 Background

While information security has always been a key enabler in personal data protection, the General Data Protection Regulation (GDPR)[3] has re-enforced it as one of the main data protection principles and a core obligation for data controllers[4] and processors[5]. According to the Regulation, 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). Taking into account the increasing use of digital and/or online data processing systems, often based on cloud services and smart devices, security risks for personal data are associated today to a great extent with 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. More recently, 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[6&7]. While big companies have the possibility to respond to and appropriately implement these frameworks, Small and Medium Size Enterprises (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. This can put in harm's way the personal data processed by SMEs, hindering at the same time SMEs' compliance with the GDPR legal obligations.

On this basis and as part of its continuous support on EU policy implementation, ENISA published in 2017 a set of guidelines for SMEs[8], acting as data controllers or processors, which aim at helping them assess security risks and accordingly adopt security measures for the protection of personal data. Those guidelines can also be of use in all cases where risk assessment is envisaged under the Regulation (e.g. Data Protection Impact Assessment, personal data breach notification, etc). Within 2017, the Agency continued its activities in the area and focused on providing further guidance on the application of the aforementioned guidelines through specific uses cases[9]. Within each use case, a personal data processing operation was identified, further discussed and then the level of risk was calculated, with the goal of providing practical examples of how data controllers/processors can make the most out of it.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[4] 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 (article 4(7) GDPR).

[5] A natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller (article 4(8) GDPR).

[6] CNIL Guide regarding security of personal data https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

[7] ICO Cyber Essentials https://www.cyberessentials.ncsc.gov.uk/

[8] ENISA - Guidelines for SMEs on the security of personal data processing https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

[9] ENISA - Handbook on Security of Personal Data Processing https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

Against this background, the Agency under its 2018 work-programme[10] advanced further this work towards the analysis of specific security measures that can be employed by controllers or processors, following the aforementioned risk assessment framework.

1.2 Scope and objectives

The overall scope of this study is to continue supporting SMEs, acting as data controllers or data processors by providing guidance on the selection of appropriate technical and organizational security measures, depending on the identified level of risk. In doing so, this study builds on experience gained from past ENISA work delivered along these lines.

This study provides an overview of well-established security practices, for the purpose of sketching the notion of "state-of-the-art" in a number of categories of measures, as they are listed in ENISA's guidelines for SMEs on the security of personal data processing[11]. In particular, the following categories have been analysed, taking into consideration specific aspects that are relevant to the processing of personal data:

- Access control and authentication.
- Incident handling and personal data breaches.
- Logging and monitoring.
- Server and database security.
- Workstation security.

The outcome of this report complements the two ENISA studies mentioned above. To this end, the study provides for a general and simple description of key security measures without providing specific technical implementation details.

The target audience of the report is mainly SMEs, acting as data controllers and data processors that can use the guidance on well-established technical and organizational measures while pursuing compliance with the GDPR. Data Protection Authorities (DPAs) might also find this analysis of interest in the context of their own data protection audit frameworks and security recommendations. This report focuses purposefully on security measures and it does not aim at making any legal analysis or assessment of compliance of specific data processing operations.

1.3 Outline

The structure of the remaining of the document is as follows:

- Chapter 2 provides an overview of the ENISA's guidelines for SMEs on the security of personal data processing, in particular the proposed security risk assessment framework.
- Chapter 3 discusses the challenges of selecting appropriate technical and organisational measures, based on the state-of the-art notion, as introduced in the Regulation.
- Chapters 4 to 9 provide an analysis of the categories of security measures mentioned earlier.
- Chapter 10 summarizes this study while providing a number of conclusions that were drawn.

(ENISA, 2018)[10] ENISA programming document 2018-2020, https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020.

[11] ENISA - Guidelines for SMEs on the security of personal data processing https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

This report is part of the work of ENISA in the area of privacy and data protection[12], which focuses on analysing technical solutions for the implementation of GDPR, privacy by design and security of personal data processing.

[12] https://www.enisa.europa.eu/topics/data-protection

2. 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. In this section, we present an overview of the approach[13] that was proposed by ENISA in 2017 towards guiding the SMEs through their specific data processing operation and supporting them in evaluating 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 to provide guidance to SMEs.

This approach is based on the five step approach, depicted in Figure 1 below.

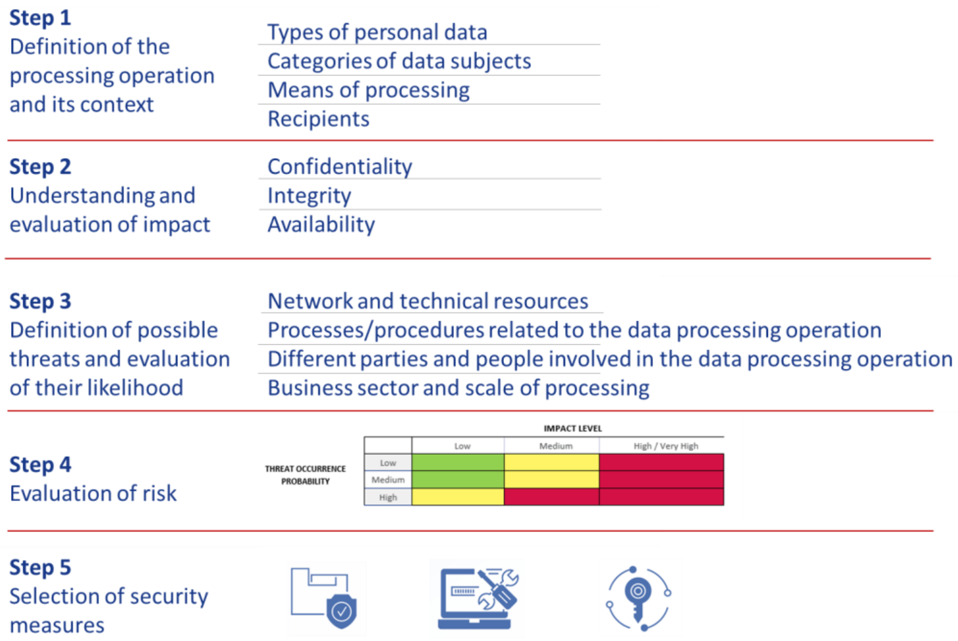
Step 1
Definition of the processing operation and its context
Types of personal data
Categories of data subjects
Means of processing
Recipients
Step 2
Understanding and evaluation of impact
Confidentiality
Integrity
Availability
Step 3
Definition of possible threats and evaluation of their likelihood
Network and technical resources
Processes/procedures related to the data processing operation
Different parties and people involved in the data processing operation
Business sector and scale of processing
Step 4
Evaluation of risk
IMPACT LEVEL
Low
Medium
High / Very High
THREAT OCCURRENCE PROBABILITY
Low
Medium
High
Step 5
Selection of security measures

Figure 1: Overview of proposed approach on evaluating the risk on personal data processing

Hereinafter, follows a brief overview of the aforementioned methodological steps. A more detailed analysis of each step is included in "Guidelines for SMEs on the security of personal data processing"[12].

2.1 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 data controller/processor 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 data processing (collection, storage, use, transfer, disposal, etc.) along with relevant aspects such as data recipients, means used for processing etc.

[13] ENISA - Guidelines for SMEs on the security of personal data processing https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

The following questions need, as a minimum, to be asked and to be clearly understood by the data controller/processor. Relevant examples and practical guidance, through use cases, can be found in [ENISA, Handbook, 2018].

1. What is the personal data processing operation?

2. What are the types of personal data processed?

3. What is the purpose of the processing?

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

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

6. Which are the categories of data subjects?

7. Which are the recipients of the data?

2.2 Step 2: Understanding and evaluating the impact

In this step, the data controller/processor is guided 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.

Due to the ad-hoc nature and diversity of personal data processing operations, only a *qualitative approach* can be used, based on the overall understanding (by the organization) of its specific data processing operation. To this end, the evaluation of the impact is based on a number of parameters, such as the type and volume of personal data, the criticality of the processing operation, special characteristics of the data controller/processor, special characteristics of the data subjects, as well as the level of identifiability of data subjects. Following this assessment, the controller is finally asked to assess the impact, based on four predefined levels, i.e. low, medium, high and very high (see Table 1).

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 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

The total impact is assessed separately for the loss of confidentiality, integrity and availability. The highest of these levels is then considered as the final result of the evaluation of the impact, relating to the overall processing of personal data.

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

A threat is any circumstance or event, which has the potential to adversely affect the security of personal data. At this step, the goal for the data controller/processor 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). Varying levels and types of threats to the confidentiality, integrity and availability of personal data could be considered in this respect.

Similar to 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 ENISA's approach, three levels of threat occurrence probability are defined, namely:

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

To simplify the process for SMEs, the ENISA's approach defines four areas of assessment for threat occurrence probability and guides the controller through them, namely:

- Network and technical resources (hardware and software
- Processes/procedures related to the data processing operation
- Different parties and people involved in the processing operation
- Business sector and scale of the processing

At the end, the threat occurrence probability is obtained as the highest of the scores obtained per area.

2.4 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 2 and Table 2 below.

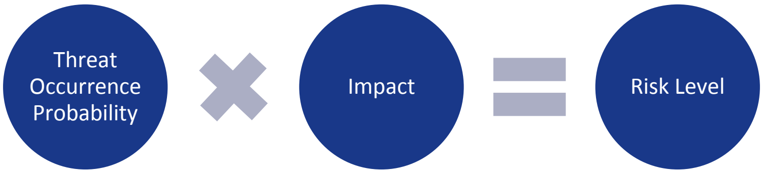

Figure 2: Final risk evaluation

		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

Legend

🟩	*Low Risk*	🟨	*Medium Risk*	🟥	*High Risk*

Table 2: Evaluation of risk

Regardless of the final result of this exercise, the data controller/processor retains the discretion to adjust the obtained level of 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.

2.5 Step 5: Selection of appropriate security measures

Following the evaluation of the risk level, the data controller/processor can proceed with the selection of appropriate security measures for the protection of personal data. Two broad categories of measures, organizational and technical ones, which are further divided in specific categories, are considered (Table 3). In principle, they follow the categorization given in ISO/IEC 27001 Annex A and ISO/IEC 27002.

Organizational Security Measures Categories	
Security management	
	Security policy and procedures for the protection of personal data
	Roles and responsibilities
	Access control policy
	Resource/asset management
	Change management
	Data processors
Incident response and business continuity	
	Incidents handling / Personal data breaches
	Business continuity
Human resources	
	Confidentiality of personnel
	Training

Technical Security Measures Categories	
Access control and authentication	
Logging and monitoring	
Security of data at rest	
	Server/Database security
	Workstation security
Network/Communication security	
Back-ups	
Mobile/Portable devices	
Application lifecycle security	
Data deletion/disposal	
Physical security	

Table 3: Overview of categories of security measures

Under each category, the measures are further presented per risk level (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 the high level of risk. Measures presented under the high level (red) are not applicable to any other level of risk

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[14], the NIS Directive[15], the Payment services Directive (PSD 2)[16] etc.

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

[15] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:194:TOC

[16]Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

3. Selecting technical and organisational measures

As mentioned in Chapter 2, the security risk assessment is the first step towards the adoption (by the controller or processor) of technical and organisational measures, which, according to article 32 GDPR, should be appropriate to the risk presented. Once the risk level has been established, the controller or processor should choose (among the pool of available measures) those that are best suited to mitigate the risks for the specific data processing operation.

This Chapter aims to refer briefly to the challenges of selecting appropriate technical and organisational measures, as well as to serve as a general introduction to the detailed descriptions of specific security measures categories in the following Chapters.

3.1 Choosing the best suited measures

Besides considering the risks of the data processing operation, GDPR sets as a condition for the choice of security measures (by the controller or processor) two additional important parameters: a) the *state-of-the-art* and b) the *costs of implementation* of relevant measures.

In particular, article 32 GDPR states that:

'*Having regard to the state of the art and the costs of implementation …., the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, …'.*

The notion of the state-of-the-art relates to the most recent stage of technological development, or otherwise the stage that incorporates the newest possible features and functionalities. The cost of implementation is clearly linked to the state-of-the-art, as technical solutions also need to be applicable in practice. In that sense, costs should be interpreted both in terms of budget, as well as in terms of human resources required for implementation of specific security measures.

By setting these requirements (state-of-the-art and costs), which greatly depend on the dynamics of technology and business processes at any given time, as conditional ones for the protection of personal data, GDPR aims at retaining options open to accommodate improvements over time, rather than setting a deterministic level of security that would inevitably become obsolete. For data controllers and processors, this provision can be perceived as an indicator for GDPR compliance being a long-term commitment rather than something static. At the same time, it also implies a need for monitoring of advances in technology and the evolvement of the cyber threat landscape.

However, defining the state-of-the-art is not trivial. First of all, it is not always evident what can be considered as 'state-of-the-art' or, in other words, what is the highest possible level of protection that a specific technology can offer. Moreover, a technique or technology that today provides a certain level of protection will not necessarily continue to do so in the future. Consider for example the case of cryptographic algorithms. Several have already been proven as flawed or weak (for example DES, 3DES, Sha1) and rapid IT developments, such as Quantum computing, are believed to render, even if not in the near future, additional cryptographic algorithms insecure.

Taking into consideration the aforementioned aspects, the selection of the appropriate technical and organisational measures is not always a straightforward decision, especially for SMEs that do not always have a deep level of relevant knowledge and/or resources.

3.2 Guidance on basic categories of security measures

In order to shed some light for SMEs on the selection of possible security measures, this report aims to provide in simple words some basic measures that can be adopted on the basis of the level of risk, as well as the state-of-the-art. Having said that, it is important to note that this description is not exhaustive and does not claim to prescribe the state-of-the-art, but rather to provide some general guidance on the matter. Moreover, not all categories of security measures (as mentioned in Table 3 – Section 2.5) are analysed in the report. In particular, the focus was mainly put on technical measures and especially in the following broad categories of measures:

- Access control and authentication.
- Incident handling and personal data breaches.
- Logging and monitoring.
- Server and database security.
- Workstation security.

For each of the above-mentioned categories, in the following Chapters (4 to 9) firstly a short description is provided and then specific measures are discussed, based on list of measures provided in (ENISA, 2017). These measures are presented in accordance with the risk level (low, medium, high), as this is obtained by the controller or processor, following a risk assessment approach.

In order to support understanding of the different measures, references to specific examples are sometimes made, often based on the use cases presented in (ENISA, 2018).

4. Access control and authentication

4.1 Overview

Access control and authentication are mostly preventive measures, as they aim to stop/prevent unwanted or unauthorized activity from occurring; they represent a critical checkpoint for information security governance, while establishing and protecting planned access to information/data. All authorized and most of the unauthorized access will directly rely on the security of in-place access control and authentication measures. Access control and authentication measures are therefore crucial to ensure the confidentiality of the personal data processed, as well as their integrity and availability.

Access Control

Access control ensures that authenticated users access only information they are entitled to. A number of different governance models can be adopted to implement access control measures, among which the most widely ones used today are:

1. **Discretionary access control (DAC):** is a model in which each resource is linked to access control properties, completely defined by the resource owner, defining which actions each user is allowed to perform for each resource. This model best fits in de-structured environments in which roles and responsibilities are not fully detailed.

Example: While processing customers' personal data for marketing purposes, an employee of an SME may upload such data to on-line cloud storage provider to allow exchanges with third party users having a legitimate business need but no access to the organization information systems. For instance, this could be the case of a specific service request such as a print service and delivery service. Through DAC, the employee is able to specify which data, for each external to the organization user, and what action(s) are permitted. It is evident that DAC provides users with an advanced flexibility on setting up desired access control properties, however it relies heavily on user's awareness and understanding of risk sensitivity. In addition, through DAC the organization cannot fully enforce an overall access control policy.

2. **Role based access control (RBAC):** is the most balanced model, based on which access is granted relying on a user's role and implements key security principles, such as "least privilege" and "separation of duties". This model best fits in environments with uniform roles and responsibilities that can be easily related with a limited number of access profiles.

Example: In the context of a hospital information system, each actor (doctor, nurse, administrative personnel) is assigned to different roles, which also have different privileges (e.g. the doctor can access the medical data, whereas the administrative personnel can only access the administrative/financial data). Through such an approach, the organization can enforce an overall access control policy based on the need-to-know principle. However, it does not offer directly granular access (to the same data item) and the access rights of each role have to be maintained and updated.

3. **Attribute Based Access Control (ABAC):** it is the most recent model, in which each resource and user are assigned a series of attributes that can be combined within access policies that can

employ logical rules. ABAC has been identified as a Privacy Enhancing Technology in ENISA's report on Big Data. This model best fits in environments with a variety of roles and responsibilities that cannot always be easily related with a specific access profile or when more granular access to data is required.

Example: In the context of an SME's human resources department, only those financial officers having a specific attribute (e.g. finance controller) may access financial data of employees. Therefore, while all designated HR staff can access employee records, the part related to financial data is accessible only to those with the specific attribute. Through such an approach, the organization can enforce an overall granular access control policy based on the need-to-know principle and access privilege maintenance is easier. However, the initial deployment on identification and assignment of appropriate attributes is often complex.

Access control systems can be implemented either individually on each information system or in a centralized manner; the latter can support access control requirements across multiple information systems in an organization. In such a case however, controls listed within this category have to be applied to every access control system to be effective. Access control systems are strongly related to the management of the IT system users. IT system access administrators should be enabled to timely reflect every organizational change into an adjusted access profile regarding each user (e.g. consisting in: creation of newly hired/contracted users, modification of its access privilege according to a job change, periodically reviewing the assigned privileges and deleting/disabling terminated users).

Authentication

Authentication determines whether the identity claim performed by a user is authentic. Authentication techniques usually require user identification plus one or more of the following authentication factors:

- Something known by the user (such as passwords, PINs).
- Something possessed by the user (such as tokens, smartphones, cards).
- Something that is a user characteristic (such as biometric features or behaviours).

Once an authentication process is successfully completed, specific privileges will (or will not be) granted to the claiming user on a set of information systems. This depends both on the user's profile and on the scope of the authentication system. A user's profile includes a set of permissions which are related directly to the access control governance model and should include the least privileges related to the task. The scope of the authentication system can be as small as a single information system or as wide as a whole organization if proper single sign-on mechanisms have been deployed.

4.2 Recommended measures

As mentioned in the (ENISA, 2017), access control and authentication are basic security measures for the protection of personal data. In particular, ENISA's guidelines recommended the following list of measures (appropriate to the risk presented – in traffic light system).

Identifier	Measure Description	Level of Risk
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.	

Table 2: Access control and authentication measures

Measure K.1, above is related to the general application of an access control policy within the organisation, as well as proper user management. Measure K.2 is a subcategory of K.1 related to the use of common accounts. Measure K.3 mandates the need for a minimum authentication mechanism, i.e. the use of username/passwords and the adoption of relevant password policy. Measure K.4 calls for the existence of a configurable level of complexity for these passwords. All aforementioned measures (K.1-K.4) are relevant to all categories of risk level (low, medium, high).

On top of measures K.1-K.4, measure K.5 calls explicitly for a specific, well-defined and documented password policy. Measure K.6 also mandates the use of hashed passwords. These measures are needed at least for risk levels medium and high. Measure K.7 calls for two-factor authentication; measure K.8 for device authentication for high level of risk.

In the next sub-sections, each one of these measures is described in more detail.

4.2.1 Access control policy and user management

Measure K.1: An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, modifying, reviewing and deleting user accounts.

As discussed earlier, access to all types of data, and therefore to IT systems and related software, should be mediated by an access control system. Contemporary endpoints and software provide local access features that support user accounts management. These features should always be enabled. The scope of this measure is to support all organizations, and specifically SMEs, to select a suitable access control system (based on their business model and the risks related to the data processing operation) and taking into account proper user management policies. To this end, the following elements need to be considered:

1. Most but not all of modern access control systems support selection between the governance models listed earlier. The choice of model should be made in conjunction with the access control system which, in turn, is often provided by the information system vendor. Careful consideration must be given before choosing the access control system(s) that are to be used and/or their configuration. Nowadays, most operating systems can in fact be configured to support different access control governance models, starting from a basic DAC up to the most refined ABAC.
2. Wherever possible, centralized access control systems should be deployed, allowing for a more effective implementation and easier day-to-day management. A centralized approach is less prone to errors and omissions and allows for an easier verification of access privileges while it can introduce additional deployment and set-up costs. Open LDAP[17] is an open-source solution implementing this with the advantage of also being operating system independent.

Example: An SME manages business relationships through a centralized CRM software via extranet, directly connected to the CRM suppliers' platform. As there is a need to manage the access of third-party vendors and suppliers to the supporting IT systems, the access control system must allow for creating, approving, reviewing and deleting user accounts of external users (as well as internal), based on their relevant access authorisations. This process needs to be regularly reviewed and refined.

3. When several access control systems are maintained, consideration should be given to linking them in a single sign-on context. Prior to such a deployment though, aspects related to possible data interconnection or data isolation requirements need to be taken into account.

Note: Having a formal access control policy in place, approved by the organization's management and defining how the access control system should operate, using which controls on what profiles is a universally recommended enhancement to this control, as specific procedures/workflows/templates for user registration, modification and termination are[18].

4.2.2 Use of common accounts

Measure 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.

[17] https://www.openldap.org/

[18] See also (ENISA, 2017), measures C.1 – C.4 (category: Access Control Policy).

All IT systems provide for user accounts, which should be assigned to a unique user in order to allow for the definition of specific access control privileges and to track all actions carried out by a single individual. This is central to all types of access control systems and is essential for the security of data. If more than one access control system is used, then the user has to be present (and correctly profiled) wherever he/she has an access need, with considerable replication effort.

To this end, the following elements need to be considered:

1. Common user accounts, especially if they have known default values, need to be disabled. Should there is a need for shared user accounts (e.g. in functional accounts) then they must be shared only across users with complementary roles. In such case, the ability to reconstruct which individual has been using the account at any given moment (e.g. via log files or user tracking) is needed.
2. A unique identifier should be permanently associated with each system's user and never be reused for others. This would imply not deleting users' accounts but only disabling them, so as to allow for long-term traceability of users actions.
3. Registries can be used to log and monitor which individuals are using a common user account.
4. Periodic reviews should be carried out to ensure the state of default user accounts. Such accounts could also be accidentally triggered by an update or a configuration change even if they were originally removed[19].
5. Having a formal procedure in place defining the criteria for user creation is a recommended enhancement to this control.

Example: In a hospital, there are programs facilitating the employment of nurses and doctors. For short term internships the IT department decides to assign to staff shared accounts. Consequently, all trainee nurses share the same account, and the same applies to intern doctors for each specialization. This is a clearly a bad practice, since in increases the risks of unlawful access and unauthorized modification to the patients' health data. The workaround solution to forward any actions performed by trainees to the reference doctor for approval or cross check can potentially mitigate risks, but it is not sufficient to be fully accountable.

4.2.3 Minimum authentication mechanism

Measure 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.

[19] See also (ENISA, 2017) , categories Access Control Policy and Logging and monitoring

An access control system (see measure K.1) should be configured to require user authentication prior to granting any access to the system and consequently ensuring that only authorized users can access the system[20].

User authentication is usually (but not exclusively) performed by presenting to the access control system a set of access credentials which are ultimately linked to a user profile. In addition to the user account identifier (commonly named "userid") there are other categories of elements that can be included in the required access credentials (see measure K.7), the simplest of which is something known by the user, such as a password. Therefore:

1. Each access control system should be configured to require and verify at least an additional element to the userid (like a password) before authenticating a user.
2. The access control system should also be configured to verify that the additional element to the userid respects a series of constraints ensuring their security qualities. For a password those constraints include complexity (see measure K.4), length, age, etc (see measure K.5).
3. Having a formal access control policy in place, approved by the organization's management, and defining how the access control system should be configured for authenticating users with different profiles is a universally recommended enhancement to this control.

4.2.4 Password complexity

Measure 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.

The use of complex passwords can offer additional resilience against password guessing attacks aimed at obtaining unauthorized access. It can be configured as a mandatory requirement within most of access control systems (see measure K.1). Adequate consideration should be given to the fact that more stringent complexity requirements will end up frustrating users or making them write down passwords, a practice which will eventually weaken the effectiveness of passwords. Rules for requiring passwords complexity are usually enforceable by all access control systems even if they can vary in the given choice of available options. Usually they can require the presence characters belonging to set of characters such as:

- lower-case alphabetic ("abcdef" …);
- upper-case alphabetic ("ABCDEF" …);
- numeric ("01234" …);
- special ("!_$#à§@" …);

Required password complexity levels should be defined (and formalized as stated in measure K.5) respecting the following rules:

1. A baseline complexity requirement to use both alphabetic and numeric sets of characters, that can be increased to 3 or more instantiations for additional security.
2. Hard to guess (e.g. present in language / common passwords dictionaries) passwords are selected; passwords feature no common paths (e.g. same character repetitions, username variations).

[20] See also (ENISA, 2017), measures C.1 – C.4 (category: Access Control Policy)

3. After a specified number of unsuccessful authentication attempts (see measure K.5), the user account is suspended or challenged (by prompting the user to provide additional information), thus limiting significantly the password guessing opportunity for an attacker.

Note: Depending on password complexity the needed combinations for a brute-force guessing can substantially vary, as depicted in the following cases.

1) an 8 lower-case alphabetic characters password has 26^8 possible combinations
2) a 8 lower and upper case alphabetic characters password has 52^8 possible combinations, which is 256 times more
3) an 8 lower and upper case and special characters password has 85^8 possible combinations, which is 13048 times more than the first case and 51 times more than the second case
4) an 11 lower-case alphabetic characters password has 26^{11} possible combinations, which is even more than the last case.

Further guidance on passwords can be found in Section to 4.2.6 - Password storage.

4.2.5 Password policy

Measure 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.

To counter password guessing attacks, constraints together with complexity requirements considered in measure K.4, are usually depicted within one or more password policies. Such policies should be defined and implemented taking into account each IT system and related information security requirements, following the aspects discussed below.

1. Where passwords or equivalent elements are used, the related access control system should be configured to dictate at least:
   a) a required password length (suggested minimum: 8 characters);
   b) an expiry date (suggested maximum: 90 days);
   c) a required history (suggested minimum: different from 4 previous ones or even no reuse);
   d) a required complexity (see measure K.4).
2. Other assurance elements that should be configured in the access control system to enhance the control can include blocking the user account after unsuccessful attempts (suggested minimum: 6 unsuccessful attempts).
3. Adopted password policies should guide and support users to effectively manage their accounts' passwords.
4. Different password policies can be established to access systems performing different processing operations.

4.2.6 Password storage

Measure K.6: User passwords must be stored in a "hashed" form

IT systems should not be configured to allow storage of cleartext passwords in any form since they could then be easily compromised. Contemporary access control systems use cryptographic hashing techniques to mitigate this risk. A password hash is in fact the result of a non-reversible transformation function applied on the password. Although being non-reversible, there are still attack techniques like collision-based attacks that could compromise the passwords.

Particularly for operating systems, network appliances and, whenever applicable, applications, passwords should follow conditions that include the following:

1. Using robust-proven and known-weaknesses-free hashing algorithms to protect password storage while avoiding others. Some examples of hashing functions to be avoided (as per mid-2018, the list will inevitably extend in time) are RC4, MD4, MD5, SHA-160.
2. Hashing functions security should be enhanced by adding a key or random data, which is widely referred to as "salt". In most cases it is a random value added to the passwords, to avoid potential password attacks based on inherent characteristics of hashing functions themselves. This addition should not substitute the complexity of the password (as described earlier) and the robustness of the salting is heavily dependent on the implementation.
3. Stored passwords, even when robust keyed or salted hashing is deployed, should not be accessible by users.

Example: The passwords of administration and accounting users in an SME are stored in a hashed form.

The users Mary and Tom had chosen as passwords "fin@ncE" and "4ccounting". These passwords were stored, using SHA-256 as "b04b5c69fd20bcb378544665f15535ca6c417b459865ed69bec1209c7fecb6d9" and "2d83067a2b3d6a9ad59da2f4b83c25dd0b29a2363ac13bfcee6efdf4162df344".

Following a data breach, a non-authorized person obtained access to the hashed passwords table. Using a pre-arranged listing of words, such as the entries from the English dictionary, with their computed hash, or simply searching on Google the hash digests in order to find the word that generated them, the attacker easily restored the passwords. A match is found both for Mary and Tom.

Following this incident, it was then decided to enhance the hashing function adding random data (with the use of state-of-the-art algorithm and of adequate length) that increases the difficulty for a non-authorised person to obtain the passwords. Passwords are stored separately from random data.

4.2.7 Two-factor authentication

Measure 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.

The number of required factors for each access control system should be proportionate to the sensitivity of IT systems and related information to be accessed, also taking into account the assigned privileges. In cases of higher risk, two-factor authentication (based on something possessed by the user, see also Section 4.1) is a widely adopted practice.

1. There is no specific constraint of what factors are used in order to implement a two-factor authentication, as long as they belong to different categories. Having the same category repeated twice, like a password and a PIN, is not a two-factor authentication but only a two-step authentication, which ensures a limited enhancement to security level (it is just another element to guess). Two-step authentication may still be used to authorize specific high-level actions like a password or a privilege change. Selecting all three factors together would additionally increase the security level but also slow down and make the authentication process more complex.
2. When something known by the user is among the selected factors, all considerations expressed in measures K.4, K.5 and K.6 should be applied to that factor.
3. When something possessed by the user is among the selected factors it should be something difficult to duplicate and unrelated to the device used for the access. Selecting objects that are difficult to lose (e.g. a smartphone rather than a USB stick) could be a remedy with some margin of success.
4. User specific features should exclude the direct use of biometric data unless hashing functions application results are applied first. Biometrics should be managed cautiously and after considering relevant GDPR provisions.

Example: An SME that specializes in remote monitoring of patients uses a web platform to collect and correlate all data transmitted, in order to detect deviations from the clinical protocol, and the overall health their situation. By employing two-factor authentication, authorised medical practitioners must possess and use two elements in order to gain access to the platform. The medical practitioner may enter a username and password and, before being granting access to the system, he or she receives a text message with a one-time access code to his or her mobile phone for verification. In addition, the system sends periodic validation messages to the medical practitioner, to verify that he/she still uses the same mobile phone/number and, thus, mitigate the risk of identity spoofing.

4.2.8 Device authentication

Measure K.8: Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.

In cases of high risk, specific processing activities involving personal data should not be allowed on any IT system but just on specifically authorized ones, to enforce a stronger access control. The related access control systems would need to check if the user is requesting access through an authorized IT system, comparing its configuration to a set of pre-registered ones.

In order to allow a proper device authentication, the following points should be considered.

1. Several elements can be used to identify a specific IT system, like its MAC address (less secure), its main hardware components identifiers but even installed certificates (more secure). At least one of them should be used but using several ones can enhance the overall security level.
2. A combination of several elements rather than only one allows a more effective control. Particular care should be taken in order to allow occasional but legitimate hardware modifications or device changes without unnecessarily disabling users' accesses.

This measure can be seen as an enhancement to K.7, being implemented as a "something possessed by the user" within the access control mechanism (see also measure K.1) and as such the IT system used for authentication should be managed in a more controlled manner.

Example: Within an SME that supports medically assisted procreation (MAP), processing of personal data is limited to the premises of the SME and access to the IT platform is allowed only to specific employees responsible for performing MAP. In addition, and due to the high risk of the processing operation, access to the platform is allowed only from specific devices, identified via their MAC addresses and/or network related IDs.

5. Incident Handling / Personal data breaches

5.1 Overview

An information security incident is commonly defined as a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security[21]. Personal data breaches are one very important case of security incidents involving personal data with specific regard to the compromise of their confidentiality, accidental or unlawful destruction, loss, alteration or unauthorised disclosure[22], which represents a subset of possible security events. These events are becoming increasingly important since they may provoke widespread damage and may need to be notified both to data protection authorities and data subjects in compliance with GDPR articles 33 and 34.

The incident handling category includes several reactive and corrective measures, aiming at different incident lifecycle phases. Some of those measures can be automated but most of them, considering the high variety of security incidents, would require human interaction. A well-structured incident handling approach should thus help avoiding incidents, limiting the extension or the duration of their impacts and reconstructing what went wrong, effectively enabling a "lesson learnt" approach, which is fundamental for all kinds of continuous improvement considerations. There are wide arrays of toolsets available in the market that can be used to detect incidents earlier and with increased confidence. The most widespread type of those toolsets is composed by SIEM software's performing events correlation and detecting anomalous events. The use of such tools should be evaluated independently from the measures presented in this chapter, being considered as a resource to the benefit of the incident response personnel. Additional considerations on this topic can be found in the subsequent "Logging and Monitoring" chapter.

5.2 Recommended measures

Within the (ENISA, 2017), a list of measures both for incident handling and personal data breaches was proposed (appropriate to the risk presented – in the traffic light system).

Identifier	Measure Description	Level of Risk
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.	🟨
G.4	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.	🟥

[21] ISO/IEC 27000:2018

[22] GDPR Article 4, definition (12)

Table 3: Incident handling / Personal data breaches measures

As shown in the Table 3 above, measure G.1 concerns the establishment of a full incident response plan, which is the common base for all remaining measures, completed with a personal data breach reporting action as prescribed in measure G.2. In addition to these measures, G.3 calls for the incident response plan to be documented while G.4 suggests a full recording of incident-related activities, necessary for proving or improving the situation afterwards.

In the next paragraphs, each one of these measures is described in more detail.

5.2.1 Incident response plan

Measure G.1: An incident response plan and accompanying detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.

An incident response plan should define the approach to be followed when specific situations related to the occurrence of a security incident are met. This documentation should guide all users in performing a set of pre-defined actions aimed at resolving the incident while minimizing possible impact and its duration. The incident response plan should include the following guidelines:

1. Incident response actions should be ordered in a chronological order and related to each other whenever possible. Relevant guidance documents on good practices and strategies for incident management and response are published by ENISA [23, 24]. Personal data breach handling should be part of these actions. Relevant guidance in the area has been published by Article 29 Working Party[25].
2. All actions should include how the aspect of internal and external communications should be handled, with specific attention to the escalation sequence from the first responders up to the organization's management that is in charge of taking the most complex or costly decisions (see also measure G.2 for more details).
3. Before activating any incident response procedure, the evolving status of the incident should be ascertained to a certain level of confidence. A preliminary analysis should be performed as a first action.
4. The incident response procedure should include guidance elements to facilitate the understanding and evaluation of the incident status even by non-specialized personnel. All personnel involved in any incident response procedure within the incident response plan should receive periodical training on the procedures he/she is involved.
5. To increase the effectiveness of an incident response plan and depending on the size and complexity of the organization, a temporary or permanent Incident Response Team (IRT) can be established. This team should be in charge, and thus also competent, for performing most of the operational actions included in the incident response plan and escalate to the management if needed.

[23] Good Practice Guide for Incident Management https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

[24] Strategies for incident response and cyber crisis cooperation https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

[25] Guidelines on Personal data breach notification under Regulation 2016/679 http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827

An essential part of incident handling is defining whether a security incident also qualifies as a personal data breach. The incidence response plan should provide guidance on how to detect, as well as to further deal with such cases (see also measure G.2). Some examples of incidents which would qualify as personal data breaches are as follows:

- loss or theft of a document containing personal data;
- unauthorized access to a database storing personal data;
- interception of communications including personal data;
- corruption of personal data storage;
- unwanted or unprotected communication of personal data;
- personal data protection security measure malfunctioning or failure.

Example: An employee of a clinic's (SME) call centre receives a call from a person claiming that he/she has received through email a pdf file containing blood examination results of another person, together with the corresponding payment receipt. The employee should be in position to understand that this is an incident (and a personal data breach) and appropriately escalate it to those responsible for handling such incidents (who should also be in position to immediately respond to this event). The procedure should form part of the clinic's incidence response plan; the clinic needs to appropriate communicate it to all employees.

5.2.2 Personal data breach notification

Measure G.2: An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.

A personal data breach could have serious impacts on an organization's reputation and business, apart from the "consequences" imposed by the Regulation. Therefore, incident response procedures defined in measure G.1 should always include an early decision checkpoint for reporting the incident to management and possibly to the supervisory authority and the individuals affected.

The Article 29 Data Protection Working Party has provided additional guidance on this topic[26].

Example: Continuing the previous example (Section 4.2.1), the incidence response plan of the clinic should have appropriate procedures in place for triggering the notification to the competent Data Protection Authority, as well as the data subjects concerned, following an assessment of the risk (based on relevant GDPR provisions).

5.2.3 Incident response plan document

[26] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Measure G.3: The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.

Considering its potentially high complexity and the need for involvement of different actors, the incident response plan (see measure G.1) should be documented in a clear and accessible way, taking also into account the nature of SME's business. While documenting the incident response plan, the following points should be taken into account.

1. The document should cover all likely and relevant events, including personal data breaches, that did effectively lead to a security incident in the past and the ones that could realistically do so in the future (see also Sections 5.2.1 and 5.2.2). Threat reports like ENISA's[27] or other equivalent documentation should be taken in consideration with this perspective.
2. In order to be widely applicable, the document should also include a clear description and assignment of roles and responsibilities for all action items.
3. Incident response plans should be distributed in their most recent version to all actors and entities that may be involved to incident response activities, including relevant third parties.
4. A clear and unambiguous process tree, with a default notify state, for selecting the course of mitigation actions for each event should be included, keeping it as simple and straightforward as possible. Decision and evaluation points should be reduced to the least necessary to increase effectiveness.

5.2.4 Incidents and personal data breaches recording

Measure G.4: Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.

Article 33 paragraph 5 of GDPR, dictates that "*The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article*." As such, the documentation of the breach is a direct obligation to the controller, regardless of the identified level of risk. However, the data controller/processor can elaborate further on the details and collected information of the incident/breach to also enable subsequent activities such as incident response improvement, employees' awareness raising and best practises analysis.

Each actor involved in incident response activities should be required (e.g. within the incident response procedures specified in measure G.1) to keep track of all undertaken actions in a detailed timeline. Through such a detailed record of actions performed are kept, the SME would then be able to draw experience and lessons learnt.

1. Each decision, event or information used to take a decision should be recorded. Maintaining evidence of the exact timing when all this happened or was produced is a key factor to combine records from different actors.

[27] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

2. Records of decisions, actions and event should be ideally taken in a time close to the moment they occurred to ensure their accuracy.
3. Records preserved with a documented chain custody, involving the traceability of the actor(s) involved and assurance on their integrity is expected to contribute significantly to the accuracy of provided information, especially when a legal obligation of notification to competent authorities is in place.

Example: Continuing the example of Sections 4.2.1 and 4.2.2, the clinic would have to record the incident and document all evidence regarding its handling, including notification to the Data Protection Authority and communication to the data subject, if applicable. Moreover, it should review all its relevant procedures, to identify gaps and find appropriate solutions to avoid relevant problems in the future.

6. Logging and Monitoring

6.1 General description

Logging and monitoring measures are among the most prominent ones in the security incident detection category. Their primary goal is to record events, to detect any kind of anomaly and allow for a prompt and precise action, in case it is needed. They are related to incident handling (see previous Chapter) measures since incidents are often detected first through logging and monitoring measures.

Logging concerns the capacity of information systems to track system events or users' actions, making it a mostly automated process. Monitoring often uses logging, but it is broader, since monitoring can consider several other elements that are not directly obtained through logging measures (like system status or performance aspects). Typically, an automated monitoring system, raises alerts which are then inspected by a specialized and trained human operator. The more sophisticated and well configured a monitoring system is, the less false alarms and true negatives an operator is expected to receive. Logging can be used independently from monitoring, allowing to reconstruct a course of actions or events that happened in the past. For this reason, log files should be protected against accidental and/or intentional alteration and/or deletion.

Note: Logging and monitoring should not be perceived as a way of user monitoring, tracking and profiling. Prior to implementation of this category of measures, data controllers/processors are also advised to take into account aspects of the applicable national legal labour framework.

6.2 Recommended measures

Within (ENISA, 2017), a list of measures with regards to logging and monitoring was proposed (appropriate to the risk presented – in the traffic light system) and is presented below.

Identifier	Measure Description	Level of Risk
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.	

Table 4: Logging and monitoring measures

As shown in Table 4 above, measure L.1 concerns the activation of logging facilities for data access events. Measure L.2 requires that log files include essential timestamp information and are protected against modifications (which, if absent, could easily make log files useless). On top of these measures, L.3 adds to the logged events in measure L.1 activities of highly privileged users while measures L.4 and L.5 require enhancements to log files protection and monitoring.

The absence of proposed high risks measures underlines the importance of this group of measures, hence the assignment of measures under the first two levels of risk.

In the next paragraphs, each one of these measures is described in more detail.

6.2.1 Data access logging

Measure 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).

Logging levels are often specified through progressive settings, ranging from none (nothing is produced) to debugging (everything is logged). More specifically:

1. The application layer through which personal data are processed should be set to a logging level that is appropriate to the level of risk presented. This includes access, insertion, modification and deletion.
2. Due care should be used while selecting a logging level that includes the aforementioned events but does not produce an enormous quantity of unusable and potentially costly (storage and processing wise) log files. This is a trade-off choice between security and storage/processing costs that should be addressed by senior management, taking into account the level of risk presented. Moreover, a balance between logging and the protection of data subject's personal data needs to be considered, taken into account the risks presented.
3. User login attempts (both successful and failed ones) and logout events may prove useful in conjunction with those related with accesses to data. Therefore, a logging level that also includes such events should be considered.
4. Log files should always be limited to a specific size with overwriting settings enabled since they can rapidly reach extensive dimensions and can cause system resources exhaustion. This size should be calculated (or empirically observed over time) in order to allow a retention time proportionate to log monitoring and investigation activities. Sending log files to a log concentrator as specified in measure L.2 can supersede the necessity of archiving log files locally.

Note: This measure does not exclude the privileged users, as presented in L.3 - Privileged activities logging. On the contrary, it sets out a horizontal logging baseline while L.3 describes a more detailed approach specifically for privileged users.

6.2.2 Log files timestamping and protection

Measure 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.

Information system logs should not only include details on the event that triggered them but also a detailed timestamp that allows sequencing into a timely order and reconstructing a path of related events, even on different information systems. It is then obvious that a correct time synchronization among systems is necessary, otherwise the correct order would be potentially lost. Therefore, log's timestamp should report date and time with a sufficient precision since information systems could generate different numbers of events per second.

Log files should also be protected from both accidental and/or intentional alteration as a malicious user could attempt to alter log files to prevent his/her actions from being exposed. Therefore:

1. Access to log files should be available only to those who have a solid business justification for accessing them, like internal audit or incident response team members.
2. Where a log concentrator is used for collecting log files from multiple systems, it should be managed andadministered by different personnel than the one administering the information systems, in order to avoid the possibility of conflict or covering own actions.
3. Synchronization of different logging systems should be pursued. The simplest method is to use protocols like Network Time Protocol (shortened in NTP and specified in RFC 5905[28]) with a set of configured time servers. There are several NTP servers made available by governments, research or educational institutions that can be freely used for this purpose.

Note: The protection of log file integrity should be obtained through one of several ways, the simplest of which is to calculate their cryptographic hash and digitally sign the combination of the log file and the hash. Other techniques can involve writing logs directly on access-controlled folders where no one has modification privileges (system apart) or media that cannot be physically rewritten (usually called WORM) or even sending them to a different information system for storage, that would act as a log concentrator. Such deployments are also relevant to L.4.

6.2.3 Privileged activities logging

Measure L.3: Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.

Typically, the most remarkable events on information systems are the ones caused by human interaction. Other events may be logged but typically they would be less important when attempting to reconstruct a sequence of events. To this end, the logging of actions of highly-privileged users, who can substantially modify the behaviour of an information system, is essential. System administrators or operators have the right to perform those actions, that typically also include user right management. In principle all actions performed by highly-privileged users such as administrators and system operators should always be logged. Instead of logging all actions performed by all highly privileged users, it could be convenient to

[28] https://tools.ietf.org/html/rfc5905

restrict them to the use of specific commands. In this case, all user management activities and configuration changes, including installation or removal of applications and services, should be logged.

Example: An SME provides remote monitoring of patients with chronic diseases (e.g. a specialised clinic). Highly privileged users of the clinic, with application administration tasks, can assign all other users specific access rights. One specific administrator may access, for maintenance reasons, health data and, in certain cases of system errors, he/she could also modify these data. When such actions are performed, they should be adequately logged. In a case of a dispute on the medical advice provided by a physician to a patient, it is crucial, both for accountability and integrity reasons, to provide evidence that the actions were performed by authorized personnel, as reported by the system and under their responsibility.

6.2.4 Log files integrity

Measure 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.

Since logs can potentially contain sensitive to the SME information or personal data, access to these logs should not only be restricted as specified in measure L.2 but those who perform log accesses should be themselves logged while doing so. Therefore:

1. Errors and other anomalies involving log files should be constantly monitored in order to maximize their availability. Typical situations that might cause logging errors are full disks or disk/network access errors. Unplanned logging erasures or modifications should also be considered among errors and anomalies.
2. Log files deletion should be allowed only as an exceptional condition to fulfil events like a modified retention policy or for inevitable troubleshooting reasons. In such cases, the deletion should be duly authorized and logged itself (after the removal). Log integrity protection mechanisms described in measure L.2 should be disabled in case the aforementioned exceptional conditions are met.
3. Log files should provide sufficient information on who accessed the log files.
4. High risk applications may be configured to become inactive or have reduced functionalities in case an error could hinder logging functionalities.

6.2.5 Log files monitoring

Measure L.5: A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.

Log integrity protection measures described in measure L.2 should be kept active to ensure log files do not undergo unauthorized modification. In case they stop working properly (even because of authorized conditions described in measure L.4) alerts should be timely generated and sent to responsible/designated personnel and allow for a prompt verification and monitoring of the situation. Therefore:

1. A monitoring system, able to detect errors and anomalies as required in measure L.4 but also to analyse normal logging activity, should be kept active at all times, with the capability of communications appropriate alerts and generating periodical status reports.
2. The monitoring system that processes log files should be located on a different system than the one recording the log files, both for performance and for allowing a different administration. Most of log concentration facilities can be configured for analysing log flows, verifying continuous production and correctness and much more, which can include correlation rules for log files from different sources.
3. Creation of alerts should be configured whenever any abnormal behaviour is detected and sent over through multiple channels to ensure the most immediate response. Periodical reports should be produced, highlighting such events but also possible trends in logging activities that may induce risky situation (e.g. the increase of a log source that may exhaust logging disk space).

7. Server and Database Security

7.1 General Description

Security measures presented in this Chapter, as applied to servers and database configurations, are mostly preventive ones, with the common goal of reducing both the possibility of an incident's occurrence and its consequences. Servers and databases are typically where the largest amount of information is processed or stored, making them a critical point in every network. It is advisable to keep in mind that each application can involve anything from one single server to tens of them and from none to several databases, making the context to work on quite complex one.

Servers' configuration can and should include a consistent array of security measures (including the ones for access control/authentication and logging and monitoring described in the previous Chapters) which, if correctly maintained and deployed, can ensure an adequate level of security. A key prerequisite for the effective employment of the described measures is that the server is in a *secure state*, meaning that at least that the latest patches are installed and that the server is being kept malware-free.

In this wider perspective the measures described in this section should not be considered as exhaustive but as a first, important step to secure some of the most important assets for information security. Resources to apply additional measures in this perspective can be found on hardening / secure configuration guidelines, keeping in mind that there is no perfect configuration for all servers.

7.2 Recommended measures

Within (ENISA, 2017), a number of measures applicable to servers and database configuration is included and presented below (appropriate to the risk presented – in traffic light system).

Identifier	Measure Description	Level of Risk
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 needed 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.	🟥

Table 5: Server and database security measures

As shown in Table 5 above, measures M.1 and M.2 are related to the technical and business configuration of the applications running on the servers. Measures M.3 to M.5 are related to data protection through encryption (at a software or hardware level) or pseudonymization techniques. Eventually, M.6 showcases a series among the most advanced technical data protection techniques.

In the next paragraphs, each one of these measures is described in more detail.

Note: The application of this group of measures strongly depends on the context of the SME's processing operations and whether in practice the SME has deployed such IT infrastructure (servers and databases) on its own. Should a data processor be providing such infrastructure, the obligation to deploy the appropriate list of measures has to be passed on to the processor, as for all measures where a processor is part of the processing operation.

7.2.1 Dedicated application accounts

Measure M.1: Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly

Applications and databases often need an account on the system they are installed in order to function properly. If they all use the same account, they will all be able to function properly but if this account is compromised, then everything from the operating system to the application will be so. Therefore:

1. Each application should have its own, dedicated operating system account, with as much as possible limited rights, able to perform only the activities needed. Databases should be no exception to this general rule.
2. Access to application accounts should be limited in their use and should only be allowed by specific network addresses and/or systems.
3. Access credentials relating to application users are almost inevitably known by some human users and, since they cannot usually be subject to periodical changes (otherwise applications should be periodically changed themselves at the risk of service discontinuity) they should be kept in secure custody and known by the least possible number of persons. Application credentials should still adhere to the guidelines described in measure M.4 for complexity and in measure M.5 for minimum length (see Chapter 4).
4. In addition to having different accounts for each application, it is advisable that systems are dedicated to specific application types or, if possible, just to single application roles.

7.2.2 Personal data processing minimization

Measure M.2: Database and applications servers should only process the personal data that are actually needed to process in order to achieve its processing purposes.

Applications and databases are capable of processing wide arrays of data, hence:

1. Data sent or being accessible from applications and databases should be strictly limited to the ones needed for the purpose of the processing operations. This applies even more to the case of personal data processing, due to the minimization principle (GDPR Article 5).
2. Application developers should take into account this principle from the early design phases of an application, which can constitute an important part of the data controller's/processor's "data protection by design" approach. Anonymization and pseudonymization (see measure M.5) could be also applied as a consequence of those considerations.
3. During the selection or procurement of off-the-shelf applications this parameter should also be taken into account.

This measure is directly related to GDPR Article 25 provisions with regards to data protection by design and by default, in addition or as an extension of the minimization principle as set out in the Regulation.

Example: A hospital operates a dedicated system which is connected to the National Insurance Scheme, in order to be able to retrieve and update patients' data, according to underlying legal provisions. Such a system should be dedicated, it should process only the data which is needed to be transferred and the patients identification data (name, surname, social security number) should be minimised and if possible pseudonymised using state-of-the-art techniques (see measure M.5).

7.2.3 Files and records encryption

Measure M.3: Encryption solutions should be considered on specific files or records through software or hardware implementation.

Encryption is based on complex mathematical algorithms used to transform data into an unintelligible (encrypted) form and back, with the respective use of an encryption and a decryption key that can (symmetric encryption) or not (asymmetric encryption) be the same.

Data encryption can be then considered as an additional access enforcement measure: in order to decrypt a file a key, usually significantly longer than an ordinary password, is needed. File encryption techniques can be very easily applied even manually by end-users while database encryption ones are more complex and can be implemented by the database itself or by the application using the database. Regardless of the case, there are some very important communalities shared among all those techniques, the most important of them being:

1. Encryption keys should be difficult to guess (the same considerations made within measure K.4 are valid), well protected and periodically renewed.
2. Encryption algorithms should be based on the state-of-the-art[29] and continuously monitored for possible compromise.

The most basic file 'encryption technique' is to compress files and protect them with a password. This can be handy if some files have to be shared through an untrusted channel (e.g. an email or a shared folder).

[29] Several encryption algorithms are now regarded partially or completely "unsercure" through the use of cryptoanalysis techniques in the past, resulting in their protection being significantly reduced if not completely removed.

The decryption key should ideally be known only by the intended recipient, that must obtain and store it securely. In this context, the same techniques for robust password generation and protection discsussed earlier in measures K.4 and K.5 can be used to protect encryption and decryption keys, while the secure conveyance of the key can be performed using a different channel than the one used for exchanging encrypted files. Most of the common compression software, including free ones (like PeaZip[30] or 7-zip[31]) uses strong encryption algorithms when the "password protected" option is selected for generating archives. Operating similarly to compression tools, there are others open source solutions that just perform encryption functions and can be essentially used in the same way.

Software can use the same encryption primitives (often well available as publicly distributed libraries) to write encrypted data in the database. In this case only the application would be able to encrypt and decrypt data and encryption and decryption keys should be inserted within access-protected configuration files or database tables. Most of modern databases, including open source ones like MariaDB[32], do offer a set of pre-built encryption functions. The main advantage over software encryption is that all key management functions are usually already well-defined and not need to be deployed from scratch.

Should an encryption key be leaked or otherwise compromised (or even that compromise is suspected), it should be replaced as soon as possible, both for encrypting new data and for protecting already encrypted ones.

Example: Recalling the personal data breach example of Section 4.2.1, the clinic decides (as a follow up of the breach) for any future communication of medical examinations to use encryption techniques by compressing the pdf file (containing the patients examination results) and protecting it with a password. The password is communicated to the patient either in written form (e.g. after signing the document requesting that the results are sent via email), or using a one-time password (e.g. after enrolling the patient's mobile phone when signing the same request).

7.2.4 Storage encryption

Measure M.4: Encrypting storage drives should be considered.

Storage encryption leverages the very same principles as other encryption techniques exposed in measure M.3 but applies them to part of or to entire storage systems. Anything from a logical partition of a disk or a USB key up to a storage area network can have disk encryption measures deployed on this way. The most common scenario is the full disk encryption, protecting all the allocated disk space of a specific system.

Storage encryption techniques do offer protection against different types of attacks than file or database encryption techniques exposed in measure M.3: disk encryption can help avoiding data loss in case physical disks or other media are lost or stolen. Measures M.3 and M.4 are not exclusive to each other but can be combined to achieve protection from several types of attacks. In any case:

[30] http://www.peazip.org/
[31] https://www.7-zip.org/
[32] https://mariadb.org/

1. Storage encryption should be always applied on all disks where confidential data is stored, even if only temporarily.
2. The same principles enlightened by measure M.3 on encryption algorithms and keys (M.3.1 and M.3.2) should be applied when considering storage encryption.

Several tools for disk encryption are available on the market (also for free like VeraCrypt[33] or DiskCryptor[34]) and can also be used on multiple drives at a time. Many operating systems are also offering proprietary disk encryption solutions, mainly of use for client systems but also applicable to server systems. Enterprise-level storage units also offer similar, lower level, protection features.

Disk encryption, if applied on the disk where the operating system resides, can cause a slight decrease in performance, so it is a factor that has to be considered when applied to entire servers.

Example: In the context of a medical clinic, the server where patients' comprehensive electronic health records are stored should be encrypted using robust and known weakness-free encryption algorithms. Encryption should also be imposed in the cases when patients' electronic health records are stored on USB keys or CD/DVD by physicians to be transferred outside the clinic premises.

7.2.5 Data pseudonymization

Measure M.5: Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information.

In broad terms, pseudonymisation refers to the process of *de-associating* a data subject's identity from the personal data being processed for that data subject. Typically, such a process may be performed by replacing one or more *personal identifiers*, i.e. pieces of information that can allow identification (such as e.g. name, email address, social security number, etc.), relating to a data subject with the so-called *pseudonyms*, such as a randomly generated values. Therefore:

1. Data pseudonymization should be applied to confidential data processing applications' database structure, modifying stored values and adding an association table to it. This impact should be considered before pseudonymizing existing databases.
2. Data pseudonyms should be created as fully independent from the direct identifier they replace (like using a progressive numbering) or as a cryptographic function of it. In any case it is important that pseudonyms are unique and cannot be directly reconducted to the original identifier.
3. Association tables containing both pseudonymized data and original ones should be kept under tightly controlled access, better if also including encryption, and the least number of users should be authorized to access them.
4. The application of data pseudonymization techniques should be performed on every application data to be effective. Either all personal data used by an application are protected or the measure's effectiveness could be dramatically reduced. Several applications with close interaction can be

[33] https://sourceforge.net/projects/veracrypt/
[34] https://sourceforge.net/projects/diskcryptor/

configured to work on the same set of pseudonymized data instead than using their original equivalent.

Example: Let us consider a university that utilises an e-learning platform to provide for publication of the students' grades/results in exams and other relevant information. Applying a data pseudonymization technique, in conjunction with other minimization techniques (e.g. a zip code rather than street names, a time interval rather than exact dates), students' names and demographic data may be replaced by pseudonyms, so as to minimise risks of identification of the students by unauthorised third parties (e.g. in case of a breach).

7.2.6 Privacy Enhancing Technologies

Measure M.6: Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.

There are several privacy-enhancing techniques that can be applied to the database's design and configuration in addition to other protections like encryption and pseudonymization:

1. Authorized queries can be configured to limit the elements that can be accessed by a database user, their number or the frequency of allowed operations, contributing to avoid potential data dumping actions. A tight authorization processes should be put in place to lift those limitations, even temporarily.
2. Privacy preserving queries can consist in a series of measures ranging from the simple encryption of the performed query to their design optimization not to reveal any additional personal data than the ones strictly necessary, all for limiting the disclosure of personal information in the process of querying a database.
3. Searchable encryption can allow the performance of comparison and ranking operations on encrypted data without the need of decrypting them, thus enabling a more persistent data protection limiting sophisticated in-memory attacks.
4. Differential privacy techniques, consisting in the injection of a small amount of noise in order to limit the risk of linking with background information, could also be considered.

All these techniques have the benefit of generally increasing the resilience of the databases where personal data are stored to all types of attacks at the cost of requiring more database configuration effort both at their setup and to cope with ongoing modifications that they might require during their operational life.

Their application might not be feasible on all commercially available databases but should be constantly kept under consideration, especially for new designs or deployments.

8. Workstation Security

8.1 Overview

Security measures presented in this section as applied to client workstations configurations are mainly preventive ones, with the common goal of reducing both an incident's occurrence and its consequences.

Workstations can be significantly more exposed systems than servers: they are not necessarily used by IT experts, they can usually be taken offsite with ease and function even if not connected to the organization's network. Some of them (like the ones used by higher management) might also contain the most critical data of the organization.

The workstations' configuration can and should include a consistent array of security measures (including the ones for access control/authentication and some of logging and monitoring described in the previous chapters of this document plus some additional ones) which, if correctly maintained and exercised, should ensure a sufficient security level.

Therefore, the measures described in this section should not be considered as exhaustive but as a first, important step. Resources to apply additional measures in this perspective can, as for servers, be found in hardening / secure configuration guidelines like the ones published by CIS[35], keeping in mind that there is no perfect configuration for all workstations. Indeed, this will vary depending on workstation users' needs, their physical dimension (e.g. if desktops or laptops), the organization's policies and several other aspects.

Note: Laptops should be both considered as candidates for application for mobile and portable devices and workstation security measures. Some of them could be not applicable to specific laptop models and be applicable to others, depending on their features (see also Chapter 9).

8.2 Recommended measures

Within (ENISA, 2017), a number of measures applicable to workstation security is included and is presented below (appropriate to the risk presented – in traffic light system).

Identifier	Measure Description	Level of Risk
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.	

[35] https://www.cisecurity.org/cis-benchmarks/

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	

Table 6: Workstation security measures

As shown in Table 6, measures from N.1 and N.3 are related to the limitation of users' privileges that should not be of an administrative level. Measures N.2, N.4 and N.5 are related to the baseline security configuration of the workstations. Measures N.6 and N.7 provide for higher protection levels with regard to anti-virus use and external storage devices. Measure N.8 relates to the internet connectivity of workstations processing personal data, whereas measure N.9 concerns data encryption capabilities.

8.2.1 Limited users' privileges in operating systems

Measure N.1: Users should not be able to deactivate or bypass security settings.

Workstation users should be granted only a set of local privileges on their systems, which should not allow for any modification to the configuration, including all security related settings. This should prevent both accidental and intentional decrease of the workstation's protection level by the user. Most commonly this would imply that:

1. The user shall not be granted local administration privileges on the operating system.
2. Security software (e.g. anti-virus) shall be configured to not allow for any change, deactivation or suspension of it's settings, without administration privileges.
3. System administrators should have both privileged and unprivileged user profiles and use them according to the tasks they carry out.
4. Security settings of system administrators and high level managers workstations, should be higher than the ones of ordinary users, taking into account the specificities of the system(s) and risk of the processing operations (e.g. payment of salaries, managing health records, etc).

8.2.2 Anti-virus updating (weekly)

Measure N.2: Anti-virus applications and detection signatures should be configured on a weekly basis.

Workstations should be adequately protected against viruses and, in general, malware threats especially since in most cases, user interaction (such as opening an attachment) is required. The main aspect of those measures is an anti-virus/ anti-malware software, which should be installed in a way that all devices on a network are equally protected and regular updates are warranted. The update of signatures is still of key importance as it allows the software to distinguish between trusted and potentially damaging applications/files. Consequently:

1. Anti-virus definition updates should be configured with the highest possible frequency to detect and neutralise such threats.
2. Antivirus engine updates should be carried out periodically to allow for the most up to date and effective functionalities of the application to be present on the system.
3. A trustworthy source (normally a vendor’s website) should be considered as the reference point/source for acquiring updates and access to such third party resource pool(s) should be controlled.

Note: The weekly set threshold should be considered as the minimum precautionary level just for the sake of allocating responsibilities and liabilities. In practise, the notion of N.6 should be considered.

8.2.3 Limited users’ privileges in applications

Measure N.3: Users should not have privileges to install or deactivate unauthorized software applications.

Workstation users should be granted a limited set of local privileges on their systems and , in principle, they should not be able to modify any software installed. This would prevent both having untrusted and unlicensed software installed on workstations or removing security-relevant portions of it.

As described for measure N.1, most commonly this would imply that the user is not given local administration privileges on the operating system. In addition to that:

1. Authorised software installed by default should be defined on the basis of users’ needs. Requests to install unauthorised software should be firstly authorised and approved by the administrator.
2. Software licensing practices can be used as a control to mitigate the risk of installing unauthorised software. Such an approach might introduce additional workload to the IT help desk, especially when applied to developers or other specialised categories of users who may have different needs than average users.

8.2.4 Session time-out

Measure N.4: The system should have session time-outs when the user has not been active for a certain time period.

Both desktop and portable workstations are likely to be left unattended by their users. Logging out and blocking access are practices that can be used to prevent unauthorised users from accessing the workstations. More specific:

1. Time-outs should be configured to log off users when workstations remain idle. Intervals can be set based on the risk of processing operation(s) carried out.
2. After the time-out elapses, the session can be terminated or suspended, requiring users to re-authenticate to re-establish the previous session.

A common way to implement this measure is to use the operating system screen saver, keeping care to enable passwords for re-activation. Nevertheless, multiple user timeouts can exist even at an application level, to reduce the likelihood of user session hijacking.

8.2.5 Security patching

Measure N.5: Critical security updates released by the operating system developer should be installed regularly.

Software updates and security patches are periodically released by all operating system vendors to overcome newly discovered vulnerabilities of their products. Security patches are particularly important as they can address security issues that could directly exploited and eventually compromise an IT system. Any communication regarding a security patch or a vulnerability can result in an exploitation strategy by malicious users. Patch management can follow the provisions such as the ones hereinafter:

1. Critical security patches, which often remediate high-risk issues, should be installed soon after their release. Other security patches should follow a periodic schedule that, as a good practice, should not exceed 6 months. This implies keeping two timelines for patching server systems but, since workstations are less sensible systems, they could also feature a single schedule for all security patches regardless of criticality. Using a patch management tool – possibly provided by the software vendor -- is recommended.

2. Software updates beyond security patches should be also monitored, mainly because if software loses official support it becomes vulnerable to newly discovered vulnerabilities.
3. A trustworthy source (normally a vendor’s website) should be the source of patches and updates.
4. Testing before deploying vendor’s patches to all workstations should always be performed to ensure that no business functionality would suffer disruptions.

Some vendors do not distinguish between security patches and software updates. In those cases everything should be considered as a security patch and possibly be examined for deeper evaluation before deciding the update schedule.

Example: On May 2017, multiple companies and organisations around the world were hit by variations of a crypto-ransomware widely known as WannaCry. Crypto ransomware is a type of malware that encrypts a user's data and asks a ransom (usually in bitcoins) in order to decrypt them. Microsoft had published a patch since March 2017 addressing the vulnerability that was exploited by the aforementioned ransomware, however the impact was quite significant[36].

8.2.6 Anti-virus updating (daily)

Measure N.6: Anti-virus applications and detection signatures should be configured on a daily basis.

The update of antivirus engine, similar to other software, allows to detect and address newly discovered vulnerabilities and flaws, similarly to measure N.2. Especially in medium and high risk processing operations, the updating frequency of signatures should be performed on a daily basis, which as indicated earlier is regarded as a good practice.

8.2.7 External storage use limitation

Measure N.7: It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).

External storage drives can contain significant amount of data and can thus be either intentionally or accidentally become a relevant source of personal data breaches. In order to avoid this, either:

1. The workstation's operating system or security software should be configured to prevent/prohibit writing data on external storage drives. Specific drives (e.g. encrypted) could still be considered under the access policy, following an assessment of the risk they might introduce.
2. Additional security software, usually of the Data Leakage Prevention (DLP) type, should be installed and configured to limit transfer of specifically marked data/files.

Example: Data loss prevention software, deployed in the IT system of a medical clinic might prevent files, containing health records, from being copied to USB devices.

[36] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

8.2.8 Internet access limitation

Measure 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.

While personal data processing on servers is preferred, processing on workstations can be considered provided such workstations have limited, controlled or are even deprived of internet access:

1. Workstations should have limited, controlled or even zero internet access through for example the installation of a firewall.
2. DLP security software, as described in measure N.7, could be configured to restrict the operations that can be performed on the workstation's processed personal data, limiting in particular the possibility to export them outside the workstation itself.

Example: Recalling the previous example of the medical clinic, in critical environments DLP systems, as well as email proxies can be configured in order to check any uploaded attachment from working environment. However, such options need to be checked against the relevant national or sectorial legal framework.

8.2.9 Full disk encryption

Measure N.9: Full disk encryption should be enabled on the workstation operating system drives.

M.4 measure can be leveraged to perform full-disk encryption also on workstations. In this case, the custody of the encryption keys, depending on the chosen product, can be a direct users' responsibility. See Chapter 7 for further information.

9. Mobile/Portable devices

9.1 General Overview

Security measures presented in this Chapter, as applied to mobile/portable devices, are mainly preventive ones, aimed towards reducing the possibility of a security incident/breach occurrence and mitigate its consequences.

Mobile/portable devices collectively refer to smartphones, tablets, smart watches etc. As they are not necessarily used by IT experts, they can always be taken offsite with ease, while being in addition extremely versatile in nature, featuring an ever-increasing number of information sharing features. As the limits between workstation and mobile/portable devices are gradually blurred, an organization's data, including personal data, could also processed on such devices.

The mobile/portable device configuration is not as easily manageable as server and workstations' because they were not primarily designed for business applications. Nevertheless, a suitable configuration can improve matters. A non-exhaustive list of measures is made available hereinafter. Guidelines like the ones published by CIS[37], SANS or other authoritative entities could be used for further guidance.

As users may seek to use their own mobile and portable devices at work, policy enforcers need to mitigate this type of risk along with any other risk they identify at organisational level.

Note: Laptops should be both considered as candidates for both mobile and portable devices and workstation security measures. Some of them cannot be applied on specific laptop models. Within this document, laptops are mainly considered under the workstation security group of measures.

9.2 Recommended measures

Within (ENISA, 2017), a number of measures applicable to mobile and portable devices configurations is included and is presented below (appropriate to the risk presented – in traffic light system).

Identifier	Measure Description	Level of Risk
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.	

[37] https://www.cisecurity.org/cis-benchmarks/

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.	

Table 7: Mobile and portable devices

As shown in Table 7 above, measures Q.1 and Q.2 relate to the registration and management of mobile and portable devices and are complemented by Q.3 for defining their access control requirements. Measure Q.4 describes and responsibilities requirements, while measures from Q.5 to Q.7 add configuration parameters that should be adopted on mobile and portable devices to enhance security.

Measures Q.7 and Q.8 encompass additional configuration that should be applied to mobile and portable devices used for processing confidential data. Measure Q.9 concerns encryption of personal data in mobile/portable devices.

In the next paragraphs, each one of these measures is described in more detail.

9.2.1 Device management procedures

Measure Q.1: Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.

In most cases, mobile and portable devices have been designed for personal and not for professional use. Clearly defining what can be done with such devices should be a priority. Therefore:

1. A set of rules for mobile and portable devices acceptable use should be documented and distributed to all users.
2. The rules for mobile and portable devices acceptable use should include, as a minimum, requirements such as:
    a) user responsibilities and instructions for secure physical custody of the device;
    b) instructions for appropriate use of security measures;
    c) type and amount of data allowed to be stored on the device and associated protection means;
    d) how the device should be connected with non-enterprise networks and other devices;

e) what to do in case of theft of the device or other security incident;
f) what type of monitoring and security measures are used to control the device;
g) whether and what personal use of the device (BYOD) is allowed;
h) whether and how personal devices uses are allowed.

In relation to this measure, EDPS has published a guidance document[38] on the protection of personal data in mobile devices used by European institutions, which can also be referred to as a basis for identifying relevant threats and mitigation practises.

9.2.2 Device pre-registration and pre-authorization

Measure Q.2: Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.

For devices connected to an organization's information system or parts thereof (e.g. to the e-mail), the following provisions apply:

1. Devices that are assigned to users having a business need should be allowed connectivity, subject to security and personal data protection policy provisions.
2. Remote access privileges to specific devices related to authorized users should be assigned using their registered MAC addresses, IMEI identifier (as applicable) or installed remote access certificates.
3. In case of theft, or loss of control, of the mobile or portable devices, they should be reported without delay and de-listed from the authorized ones.

As described in measure K.7, multiple factor authentication could also be leveraged to reduce the risk of unauthorized accesses even after mobile or portable device have been stolen.

9.2.3 Device access control

Measure Q.3: Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.

Additional device control measures that can be activated, in case of loss of control or theft, include the following:

1. Mobile and portable devices access control configuration should adhere and follow the good practices listed in measures K.1 to K.8. Typically, a practical solution is to extend, if possible, the operating system access control measures already in place.

[38] https://edps.europa.eu/sites/edp/files/publication/15-12-17_mobile_devices_en.pdf

2. Device access control could replace default settings e.g. one factor authentication, with a higher grade one (e.g. longer key length, two factor authentication, biometrics etc).

Some mobile and portable devices feature dedicated portions of memory that can be protected with additional access control measures.

9.2.4 Roles and Responsibilities for device management

Measure Q.4: Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.

Mobile and portable devices management should encompass technical and non-technical aspects that can potentially influence security throughout the lifecycle. This includes but is not limited to configuration and change management, patch management, security software management, incident management, monitoring and also physical assignment. Therefore:

1. All activities relating to mobile and portable devices management should be assigned to specific and defined persons or teams within the organization with respect to all employed mobile and portable devices, defining specifically related roles as needed.
2. Duly specialized IT management personnel should be in charge of the mobile and portable devices management, considering diverse features and considerations when compared to ordinary workstations.

Mobile and portable devices are often provided and managed as a service by third parties, especially for SMEs. It is important that contracts with these organizations define all the relevant responsibilities related to their management, in line with the organization’s security and personal data protection requirements.

9.2.5 Remote deletion of personal data

Measure 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.

As mobile and portable devices are prone to loss or physical theft, they organization should be able to erase organizational data/files remotely. Therefore:

1. Their configuration should allow authorized access (see measure Q.4) to remotely securely wipe personal data stored on the device. Remote wipe commands can be sent from a properly configured Mobile Device Management (MDM) platform, which can be acquired or provided as a service by a third party. Proper platform authorisation and action tracking are required to execute such a command.

2. If relevant for the processing operation, the location data of the owner of the mobile or portable device could be used to initiate a remote command e.g. wipe operation. In this case, the location data should not be perceived as a way of user monitoring, tracking and profiling. Prior to implementation data controllers/processors are also advised to take into account aspects of the applicable national legal labour framework.
3. Data erasure should be performed not just with a simple deletion command but using techniques that render the deleted files unrecoverable, typically by overwriting memory segments.

Once an MDM platform is configured, several other features or options could be activated, including remote device locking, that should be performed as a first action after receiving a theft/loss notification. There are few open-source or free MDM solutions on the market, as FLYVE[39] or some entry-level offers up to a specific (small) number of devices offered by the major MDM software producers.

This measure could be seen as redundant if device encryption (see measure Q.9) is used. It could address cases in which the device is lost or stolen powered-up and with encryption measures potentially unlocked.

9.2.6 Separation of device usage

Measure Q.6: Mobile devices should support separation of private and business use of the device through secure software containers.

In case mobile and portable device personal use is allowed by the organization (and communicated as specified in measure Q.1):

1. The device itself should be configured to ensure adequate protection to business data, which should be stored separately and unlocked only when needed to limit their unauthorized access opportunities.
2. Some mobile and portable devices operating systems feature dedicated portions of memory that can be protected with additional access control measures. Personal and business data could be allowed to be conveniently segregated this way, aligning the additional measures with the ones established for the ordinary workstations. Business data stored this way can often be additionally protected with encryption techniques, which should be configured as specified in measure M.4.

   In case the operating system does not support those functionalities, additional software for this purpose is available for all major mobile operating systems, being in some cases included as a feature within MDM software described in measure Q.5.

9.2.7 Device physical protection

Measure Q.7: Mobile devices should be physically protected against theft when not in use.

[39] https://github.com/flyve-mdm

Mobile and portable devices should also be physically protected, when applicable, in cases when they are not used, even inside the organization's premises as part of Q.1 measures. More specifically:

1. Physical locks should be used to secure laptops and tablets that have to be left unattended for a limited amount of time.
2. Screen locking measures, that are practically very similar to workstation screen savers described in measure N.4, should be set up and require authentication to be unlocked.
3. GPS-equipped devices could be linked with MDM geolocation functionalities or to equivalent dedicated software, even if this measure is not at all preventive and would not constitute a significant barrier to the potential theft. The deployment of such measure however should be implemented in a way that tracking or monitoring of the mobile device holder is prevented.

9.2.8 Device two-factor authentication

Measure Q.8: Two-factor authentication should be considered for accessing mobile devices.

1. Sharing many of workstations' features and problems, two-factor authentication should be used as described in measure K.7 to reduce risks of unauthorized accessed to potentially stolen mobile and portable devices.
2. Two-factor authentication should not only be required just at the device's power-up stage or first login and it should be repeated for unlocking it.

9.2.9 Device encryption

Measure Q.9: Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.

In case mobile and portable devices are used to store personal data:

1. Data should be encrypted as per measure M.3 or all the memory following measure M.4. In this latter case MDM solutions described in measure Q.5 or dedicated software could be used to achieve this result.
2. M.4 measure can be leveraged to perform full-disk encryption on mobile and portable devices. In this case the custody of the encryption keys, depending on the chosen product, can be a direct users' responsibility.

10. Conclusions

The General Data Protection Regulation has reinforced the provisions on security of personal data (both in substance and context) and also extends this responsibility directly to data processors. Beyond being a principle (namely a prerequisite) for the processing, security is one of the main elements of controllers' accountability. This means that compliance cannot be merely formal and based on the implementation of closed checklists, but linked to the "context" where the processing operation takes place and the actual risks. As such, it requires an engineered approach capable of striking a balance between security goals, costs and "stat- of-the-art" solutions. Considering the specific characteristics of SMEs, such as limited resources and unavailability of qualified personnel, this report builds on top of the methodological steps of presented in (ENISA, 2017) and (ENISA, 2018). It provides guidance on the selection of appropriate technical and organizational security measures, depending on the identified level of risk as well as an overview of well-established measures, towards sketching the notion of "state-of-the-art" in different categories of measures. While performing the analysis of selected measures categories, a number of conclusions and relevant recommendations were drawn and are discussed below.

State of the Art

Following the analysis of the processing operations and the calculation of the overall level of risk, data controllers/processors are called to select the appropriate security measures. However, there cannot be an all-round single best choice of a framework/standard/guide. On top of regulatory or contractual requirements, stakeholder's preferences, competence(s) and readiness, data controllers/processors are also called to act based upon the notion of state-of the art.

The research community should continue working on providing innovative technical solutions to the ever increasing security threats in the areas of security measures and privacy enhancing technologies, with the support of competent EU bodies, in terms of policy guidance and funding mechanisms.

Need for security frameworks for personal data processing

There is no "one size fits all" solution when trying to apply proper security measures. There is no single best choice of a security framework, since almost every framework today available on the market can produce adequate results if correctly implemented following an effective risk management process and with a risk based approach. Still, it is important to build coherent frameworks that can support SMEs all the way through the process, from risk assessment to the adoption of appropriate technical and organizational measures.

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 on the selection of appropriate and adequate security measures.

SMEs guidance and training

SMEs could benefit from training and awareness programs tailored for them, such as training tools to educate their employees and guidance on how to disseminate information throughout the company and apply the regulation to every aspect of their business, from the management to the infrastructure. Practical and simple guideline texts and self-service tools or materials that can be immediately used by non-experts are also very important, Examples of such possible guidance include cyber incident guidelines for SMEs, tools to assess the severity of a personal data breach, as well as tools to audit, map and make the internal flow of information compliant (self-check).

The European Commission, competent EU bodies and Data Protection Authorities shall continue communicating both the principles and compliance steps to GDPR provisions.

Practical approaches for self-evaluation

SMEs are not fully acquainted with the notion of risk from the personal data perspective and they could benefit more from a 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.

The research community and competent EU or standardization bodies, in close collaboration with regulators (e.g. Data Protection Authorities), should propose and put forward methodologies and practical ways (e.g. certification) to support data controllers/processors on assessing their level of compliance and exposure to risk.

11. Bibliography

CNIL. (2012). *Methodology for Privacy Risk Management.* CNIL. Retrieved from https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

CNIL. (2018). *Security of Personal Data.* Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf

ENISA. (2013). *Recommendations for a methodology of the assessment of severity of personal data breaches.* ENISA. Retrieved from https://www.enisa.europa.eu/publications/dbn-severity

ENISA. (2017). *Guidelines for SMEs on the security of personal data processing.* ENISA. Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA. (2018). *Handbook on Security of Personal Data Processing.* ENISA. Retrieved from https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

ENISA. (2018). *https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing.* ENISA. Retrieved from https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

ENISA
European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number TP-03-18-572-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-284-4
DOI: 10.2824/015812