Handbook on Security of Personal Data Processing

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For 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 978-92-9204-251-6, DOI 10.2824/569768

Table of Contents

Executive Summary

The General Data Protection Regulation (EU) 679/2016 ('GDPR') will be, as of 25 May 2018, the main data protection legal framework in EU directly applicable to all Member States, repealing the current Data Protection Directive 95/46/EC. Currently, businesses in the EU have to deal with 28 different data protection laws. This fragmentation is a costly administrative burden that makes it harder for many companies, particularly SMEs, to access new markets.

One of the core obligations for all businesses, including SMEs, acting either as data controllers or data processors, in GDPR is that of the security of personal data. In particular, according to GDPR security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: the higher the risk, the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk). Even if this risk-based approach is not a new concept only a few specific privacy risk assessment frameworks have been presented, focusing principally on the evaluation of risks to personal data and adoption of relevant security measures.

On this basis and as part of its continuous support on EU policy implementation, ENISA published in 2016 a set of guidelines for SMEs , 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. In close collaboration with experts from national Data Protection Authorities, each use case corresponds to a specific personal data processing operation and makes specific assumptions on the data processing environment and overall context of processing. The provided examples however focus only on security measures and do not aim at providing any legal analysis or assessment of compliance with GDPR for the specific data processing operations. While performing the analysis, a number of conclusions and relevant recommendations, targeted at different stakeholders, were drawn and are presented below.

- Competent EU bodies, EU policy makers and regulators (e.g. Data Protection Authorities) should develop practical and scalable guidelines that will be able to support and assist different types of data controllers and address specific stakeholders' communities.

- Competent EU bodies, EU policy makers and regulators (e.g. Data Protection Authorities) should promulgate a set of baseline professional skills and requirements that Data Protection Officers' should meet.

- EU policy makers and regulators (e.g. Data Protection Authorities) should define and promote scalable data protection certification schemes, that meet the needs of SMEs and empower them to achieve and demonstrate compliance.

- The research community and competent EU bodies, in close collaboration with regulators (e.g. Data Protection Authorities), should propose and put forward methodologies that combine security risk management and risk management of personal data.

- SME communities and associations, in close collaboration with competent EU bodies and regulators (e.g. Data Protection Authorities), should communicate and encourage data controllers to undertake actions towards security and privacy compliance as a competitive advantage alongside the underlying legal obligations.

1. Introduction

1.1 Background

The General Data Protection Regulation (EU) 679/2016[1] ('GDPR') will be, as of 25 May 2018, the main data protection legal framework in EU directly applicable to all Member States, repealing the current Data Protection Directive 95/46/EC[2]. Under the Regulation, one of the core obligations for all businesses, acting either as data controllers or data processors, is that of the security of personal data processing.

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

In particular, the security of personal data processing is mainly mandated in Article 32 of GDPR, which states that:

'Having regard to the state of the art and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data; (c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'

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

According to the aforementioned provisions, in GDPR security equally covers confidentiality, integrity and availability and should be considered following a risk-based approach: the higher the risk (for the rights and freedoms of data subjects), the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk). Moreover, security of processing should be regarded within the overall GDPR accountability framework for data protection, which is also risk-based and impact-based and aims to fit into the specific operational context and practices of an organization.

[1] http://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] http://eur-lex.europa.eu/eli/dir/1995/46/oj

Taking the above considerations into account, ENISA published in 2016 a set of guidelines for SMEs[3], 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. Under its 2017 work-programme, ENISA decided to continue this work by providing practical examples on the application of the guidelines by SMEs.

1.2 Scope and Objectives

The overall scope of the present report is to provide practical demonstrations and interpretation of the methodological steps of the ENISA's 2016 guidelines for SMEs[3] on the security of personal data processing. This is performed through specific use cases and pragmatic processing operations that are common for all SMEs. For each use case, the ENISA's guidelines are applied in order to assess in practice the risk (for the rights and freedoms of data subjects) and adopt the technical and organisational measures that are appropriate to the risk presented.

The target audience of the report is mainly SMEs, acting as data controllers or processors, that can use the examples as an inspiration for their own assessment of risks and adoption of security measures, while pursuing compliance with GDPR. Data Protection Authorities (DPAs) might also find the use cases of interest in the context of their own data protection audit frameworks and security recommendations.

It should be noted that, although all types of data processing systems are covered by ENISA's 2016 guidelines, this report is mainly focused on electronic personal data processing by SMEs, which is based on IT networks and systems, as well as new digital technologies (e.g. cloud computing, mobile devices, etc.).

The report focuses explicitly on security measures and does not aim at making any legal analysis or assessment of compliance of specific data processing operations.

1.3 Methodology

The report was supported by an expert group, comprising of Georgia Panagopoulou (Hellenic Data Protection Authority) and Giuseppe D'Acquisto (Italian Data Protection Authority). A number of processing operations was identified as the most typical ones or the ones that are met more often for the majority of SMEs and was then validated, to the extent possible, with relevant data controllers.

1.4 Structure

The structure of the document is as follows:

- Chapter 2 provides an overview of the methodological steps on the evaluation of security risks by SMEs, as already proposed in 2016.
- Chapters 3 to 7 present the selected use cases, with an analysis of the each processing operation and calculation of the overall level of risk, based on the methodological steps described earlier.
- Chapter 8 draws a number of final observations and conclusions with regard to the implementation of the proposed approach by SMEs.

The report complements previous ENISA's work in the fields of privacy and security of personal data[4].

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

[4] For more information, see: https://www.enisa.europa.eu/topics/data-protection

2. Risk assessment and security measures for personal data

ENISA, in its 2016 guidelines[5], presented a simplified approach that can guide the SMEs (acting as data controllers or processors) through their specific data processing operation, supporting them in evaluating the relevant security risks and accordingly adopting security measures.

In this chapter we provide a short overview of ENISA's 2016 guidelines that will be used in the rest of the report for providing practical examples. We also introduce the notion of 'use cases' upon which the examples on data processing scenarios will be built.

2.1 Methodological steps overview

The ENISA's guidelines for SMEs propose an approach on evaluation of risk, which is based on four steps, as follows:

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

Following the evaluation of risk, the SMEs can adopt technical and organizational security measures (from a proposed list) that are appropriate to the level of risk.

2.1.1 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 in order to define the boundaries of the data processing system (under assessment) and its relevant context. To support SMEs in defining the processing operation a set of questions is provided.

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?

While answering these questions, an SME needs to consider the various phases of the data processing (collection, storage, use, transfer, disposal, etc.) and their subsequent parameters.

2.1.2 Step 2: Understanding and evaluating impact

Based on the analysis of Step 1, the data controller at this stage must assess the impact on the fundamental rights and freedoms of the individuals, resulting from the possible loss of security of the

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

personal data. Four levels of impact are considered (Low, Medium, High, Very High) as shown in Table 1 below.

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

Table 1: Levels of impact description

The evaluation of impact is a qualitative process and a number of factors need to be considered by the data controller, such as the types of personal data, criticality of the processing operation, volume of personal data, special characteristics of the data controller, as well as special categories of data subjects.

In order to support the controller in this process, Table 2 can be used to assess separately impact from loss of confidentiality, integrity and availability.

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

NO	QUESTION	EVALUATION
I.1.	**Please reflect on the impact that an unauthorized disclosure (loss of confidentiality) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.**	□ Low □ Medium □ High □ Very high
I.2.	**Please reflect on the impact that an unauthorized alteration (loss of integrity) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.**	□ Low □ Medium □ High □ Very high
I.3.	**Please reflect on the impact that an unauthorized destruction or loss (loss of availability) of personal data - in the context where your business activity takes place - could have on the individual and express a rating accordingly.**	□ Low □ Medium □ High □ Very high

Table 2: Impact evaluation questions

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

At this step, the scope for the data controller 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).

To simplify this process, a number of assessment questions have been defined, which aim at making the SMEs aware of the data processing environment (that is directly relevant to the threats). As such, they relate to four main dimensions of this environment (assessment areas), 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**

Table 3 below summarizes the questions related to the assessment of threat occurrence probability.

A. NETWORK AND TECHNICAL RESOURCES		
1.	**Is any part of the processing of personal data performed through the internet?**	When the processing of personal data is performed fully or partially through the open Internet, possible threats from external online attackers increase (e.g. Denial of Service, SQL injection, Man-in-the-Middle attacks), especially when the service is available (and, thus, traceable/known) to all internet users.
2.	**Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?**	When access to an internal data processing system is provided through the internet, the likelihood of external threats increases (e.g. due to external online attackers). At the same time the likelihood of (accidental or intentional) misuse of data by the users also increases (e.g. accidental disclosure of personal data when working in public spaces). Special attention should be given to cases where remote management/administration of the IT system is allowed.
3.	**Is the personal data processing system interconnected to another external or internal (to your organization) IT system or service?**	Connection to external IT systems may introduce additional threats due to the threats (and potential security flaws) that are inherent to those systems. The same applies also to internal systems, taking into account that, if not appropriately configured, such connections may allow access (to the personal data) to more persons within the organization (which are not in principle authorized for such access).
4.	**Can unauthorized individuals easily access the data processing environment?**	Although focus has been put on electronic systems and services, the physical environment (relevant to these systems and services) is an important aspect that, if not adequately safeguarded, can seriously compromise security (e.g. by allowing unauthorized parties to gain physical access to the IT equipment and network

		components or failing to provide protection of the computer room in the event of a physical disaster).
5.	**Is the personal data processing system designed, implemented or maintained without following relevant best practices?**	Poorly designed, implemented and/or maintained hardware and software components can pose serious risks to information security. To this end, good or best practices accumulate the experience of prior events and can be regarded as practical guidelines of how to avoid exposure and achieve certain levels of resilience.
B. PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA		
6.	**Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?**	When roles and responsibilities are not clearly defined, access (and further processing) of personal data may be uncontrolled, resulting to unauthorized use of resources and compromising the overall security of the system.
7.	**Is the acceptable use of the network, system and physical resources within the organization ambiguous or not clearly defined**	When acceptable use of resources is not clearly mandated, security threats might arise due to misunderstanding or intentional misuse of the system. The clear definition of policies for network, system and physical resources can reduce potential risks.
8.	**Are the employees allowed to bring and use their own devices to connect to the personal data processing system?**	Employees using their personal devices within the organization could increase the risk of data leakage or unauthorized access to the information system. Moreover, as devices are not centrally controlled, they may introduce additional bugs or viruses into the system.
9.	**Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organization?**	Processing of personal data outside the premises of the organization can offer a lot of flexibility, but at the same time introduces additional risks, both related to the transmission of information through possibly insecure network channels (e.g. open Wi-Fi networks), as well as unauthorised use of this information.
10.	**Can personal data processing activities be carried out without log files being created?**	The lack of appropriate logging and monitoring mechanisms can increase intentional or accidental abuse of processes/procedures and resources, resulting to the subsequent abuse of personal data.
C. PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA		
11.	**Is the processing of personal data performed by a non-defined number of employees?**	When access (and further processing) of personal data is open to a large number of employees, the possibilities of abuse due to human factor increase. Clearly defining who really needs to access the data and limiting access only to those persons can contribute to the security of personal data.
12.	**Is any part of the data processing operation performed by a contractor/third party (data processor)?**	When the processing is performed by external contractors, the organization may lose partially the control over these data. Moreover, additional security threats may be introduced due to the threats that are inherent to these contractors. It is important for the

		organization to select contractors that can offer a high level of security and to clearly define what part of the processing is assigned to them, maintaining as much as possible a high level of control.
13.	**Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?**	When employees are not clearly informed about their obligations, threats from accidental misuse (e.g. disclosure or destruction) of data many significantly increase.
14.	**Is personnel involved in the processing of personal data unfamiliar with information security matters?**	When employees are not aware of the need of applying security measures, they can accidentally pose further threats to the system. Training can greatly contribute to making employees aware both of their data protection obligations, as well as the application of specific security measures.
15.	**Do persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?**	Many personal data breaches occur due to the lack of physical protection measures, such as locks and secure destruction systems. Paper based files are usually part of the input or the output of an information system, can contain personal data and should also be protected from unauthorized disclosure and re-use.
D. BUSINESS SECTOR AND SCALE OF PROCESSING		
16.	**Do you consider your business sector as being prone to cyberattacks?**	When security attacks have already taken place in a specific business sector, there is an indication that the organization would probably need to take additional measures to avoid a similar event.
17.	**Has your organization suffered any cyberattack or other type of security breach over the last two years?**	If the organization has already been attacked or there are indications that this might have been the case, additional measures need to be taken to prevent similar events in the future.
18.	**Have you received any notifications and/or complaints with regard to the security of the IT system (used for the processing of personal data) over the last year?**	Security bugs/vulnerabilities can be exploited to perform attacks (cyber or physical) to systems and services. Security bulletins containing important information regarding security vulnerabilities that could affect the aforementioned systems and services should be considered.
19.	**Does a processing operation concern a large volume of individuals and/or personal data?**	The type and volume of personal data (scale) can make the processing operation attractive to attackers (due to the inherent value of these data).
20.	**Are there any security best practices specific to your business sector that have not been adequately followed?**	Sector specific security measures are usually adjusted to the needs (and risks) of the particular sector. Lack of compliance with relevant best practices might be an indicator of poor security management.

Following this approach, the level of threat occurrence probability can be defined for each of the assessment areas, as follows:

- Low: the threat is unlikely to materialize.
- Medium: there is a reasonable chance that the threat materializes.
- High: the threat is likely to materialize

Tables 4 and 5 can then be used to document the threat occurrence probability for each assessment area and accordingly calculate its final value.

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

Table 3: Assessing threat occurrence probability per area

OVERALL SUM OF THREAT OCCURRENCE PROBABILITY	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 -12	High

Table 4: Evaluation of threat occurrence

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

2.1.4 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 (Table 6).

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

Legend

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

Table 6: Evaluation of risk

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

2.1.5 Step 5: Security measures

Following the evaluation of the risk level, the SME can proceed with the selection of appropriate security measures for the protection of personal data.

The ENISA guidelines consider two broad categories of measures (organizational and technical ones), which are further divided in specific subcategories. Under each subcategory measures are 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 high level of risk. Measures presented under the high level (red) are not applicable to any other level of risk.

Annex A: presents the list of proposed measures per risk level.

It should be noted that the matching of measures to specific risk levels should not be perceived as absolute. Depending on the context of the personal data processing, the organization can consider adopting additional measures, even if they are assigned to a higher level of risk. Furthermore, the proposed list of measures does not take into account other additional sector specific security requirements, as well as specific regulatory obligations, arising for example from the ePrivacy Directive[6] or the NIS Directive[7]. In an attempt to further facilitate this procedure a mapping of the proposed group of measures with the ISO/IEC 27001:2013[8] security controls is also included.

2.2 Use cases and approach of the report

As already mentioned, this report provides further guidance on the application of ENISA's guidelines (section 2.1) based on use case scenarios ('use cases'). Each use case corresponds to a specific personal

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

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

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

data processing operation and makes specific assumptions on the data processing environment and overall context of processing.

To this end, within the context of EU SMEs, a number of processing operations have been identified. These processing operations vary from Human Resources (HR) related processes, provision of goods, marketing and physical security/access control. In addition to these general categories, some specific use cases from the health and education sectors are considered.

For each use case, a description of the processing operation is provided, depicting the assumptions that were made and the specificities that were taken into account. Then the evaluation of risk is performed, on the basis of the assumptions made within the description and throughout the various steps. Specific parameters that could alter the overall risk are also mentioned in certain cases. Following the risk evaluation, the appropriate (to the identified level of risk) security measures can be adopted based on Annex A:.

The calculation of risk for each use case should only be seen as an example of the application of ENISA's guidelines under the specific example scenario (and relevant assumptions made).

It cannot be regarded as an *a priori* applicable to the related data processing operations.

The data controller is advised to start with the examples provided and further carry out the assessment based on her specific data processing context and environment.

The use cases focus only on security measures and do not aim at providing any legal analysis or assessment of compliance with GDPR for the specific data processing operations.

To this end, any assumptions made under the use cases are only meant to facilitate the provision of practical examples and they do not provide any indication with regard to the legality/compliance of specific data processing operations.

3. Use Cases: Human Resource Processes

A typical SME will process personal data of its' employees as part of the Human Resources (HR) activities. Depending on the nature of business activities, the size and the internal organization of an SME, the Human Recourses activities might pertain additional procedures, process more or less personal data or for different purposes. The most common processing operations that we consider in this report are: a) Payroll management, b) Leave - absence management, c) Recruitment and d) Evaluation of staff. Other operations could include Health data of staff (e.g. annual medical check-ups required by the employer, trainings of staff, etc.

3.1 Payroll management

Within the scope of this use case, we consider as an example a retail SME that processes personal data of its employees for salaries, benefits and social security. The personal data considered to be processed are: contact information (such as last and first name, address, telephone numbers,) social insurance number, taxation Identifier, date of employment, position and salary information. The processing operation is facilitated by the HR IT system, which is deployed within the premises of the SME, and the HR officer operates it. There is a specific use policy in place. However, there are no specific policies regarding data retention and destruction. Processing of personal data is limited to the premises of the company. Towards the end of each month, the HR officer submits to the financial Institutions and the social security institute statements for all employees. Although the HR officer has signed a confidentiality disclaimer, no security or data protection training has recently been performed for the SME's employees.

3.1.1 Definition of the processing operation and its context

The specific data processing operation can be detailed, as follows:

PROCESSING OPERATION DESCRIPTION	EMPLOYEES PAYROLL MANAGEMENT	
Personal Data Processed	Contact information (last and first name, address, telephone number,) social security number, taxation Identifier, date of employment, salary information	
Processing Purpose	Payroll management (payment of salaries, benefits and social security contributions)	
Data Subject	Employees	
Processing Means	Human Resources IT System	
Recipients of the Data	External	Financial Institutions
	External	Social Insurance Schemes
Data Processor Used	In-house (no data processor)	

3.1.2 Evaluating Impact

Following the approach presented in section 2.1.2, the following analysis can be made:

Loss of confidentiality

Within the scope of the employees' payroll management processing operation, as described above, the impact from loss of confidentiality is mainly related to potential unintended disclosure of income (and other relevant data) to third parties. This could expose the data subject to consequences ranging from the discomfort arising from the public knowledge of one's own private data to even, in specific cases, the potential risk of targeted attacks from thefts or money seekers. This might be more than a simple annoyance, and the impact from loss of confidentiality could, thus, be set to MEDIUM.

Loss of integrity and availability

The loss of integrity and/or availability might be in general considered as LOW, as data subjects are expected to face inconvenience (e.g. need to resubmit information or unable to receive monthly payment on time) but the problems can be quickly overcome. More serious impacts from loss of confidentiality might be set to MEDIUM if the consequences to data subjects are more persistent over time (e.g. repeatedly delaying payments of salaries); this is however not considered to be the general case in our example.

The next table summarizes the aforementioned analysis.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Low**	**Low**
	Overall Impact Evaluation	**MEDIUM**

The overall result of the evaluation of the impact is the highest identified. Therefore, the overall impact in this particular case is evaluated as MEDIUM.

Further to the assumptions made in this example, there might be cases where the overall impact could be higher from the one calculated above. An example of such case could be the:

- systematic processing of specific health/disability data (e.g. due to special privileges/working arrangements, such as extra allowances for impaired or disadvantaged employees). In such case the data controller should consider whether the impact level is set to HIGH.

3.1.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources:** The threat occurrence probability is LOW, as the system is not connected to the internet and does not allow access from internet to internal resources and other IT systems. It is assumed for this use case that unauthorized access is prevented following relevant ICT security best practices.
- **Processes/Procedures related to the processing of personal data**: The threat occurrence probability is LOW, assuming that roles and responsibilities of HR officer are clearly defined along to an acceptable use policy, processing of personal data is limited to the premises of the organization and log files are created for any processing activity.
- **Parties/People involved in the processing of personal data:** The threat occurrence probability is MEDIUM as HR officers have not received relevant information security training and it is not certain that personal data are always securely processed and/or destroyed (due to lack of relevant policies – see use case description).
- **Business sector and scale of processing:** The threat occurrence probability is LOW as the business sector of the SME is in general not considered prone to cyberattacks. It is assumed that no personal

data breach is known to have occurred in the past and the processing operation is limited only to the employees of the SME.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Low**	**1**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**Medium**	**2**
Business sector and scale of processing	**Low**	**1**
Overall Threat Occurrence Probability	**Low (5)**	

Following the aforementioned assessment, the overall threat occurrence probability is calculated as LOW.

3.1.4 Evaluation of Risk and Adoption of Security Measures.

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨 **X**	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

The overall risk for this particular case is generally considered as MEDIUM. Annex A: (A.1 and A.2) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (higher) under special conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 3.1.2).

3.2 Recruitment

Within the scope of this use case, we consider again the retail SME described in section 3.1. Staff recruitment is a process run by HR and consists of numerous organizational activities aimed at the selection of people who have specific skills or are capable of performing certain tasks. After the vacancy notice has been published, candidates are invited to submit their application electronically alongside a detailed curriculum, with the academic education and qualifications, working experience, further professional or academic training, family status, and personal details such as first and last name, address, telephone numbers, date of birth. The selection committee reviews and evaluates the applications and comes up with a list of candidates to be invited for an interview. During the interview, the selection committee members take notes on the performance of the candidate and at the end they draft a detailed report which is submitted to senior management. Processing is facilitated by an IT system which supports the submission of applications, the shortlisting of candidates and the interview reports and is operated by an HR officer.

3.2.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	RECRUITMENT	
Personal Data Processed	**Academic education and qualifications, working experience, further professional or academic training , family status, first and last name, address, telephone numbers, date of birth, interview notes/report**	
Processing Purpose	**Managing candidate selection for recruitment**	
Data Subject	**Recruitment Candidates**	
Processing Means	**Recruitment IT platform**	
Recipients of the Data	**Internal**	**Senior Management**
Data Processor Used	**In-house (no data processor)**	

3.2.2 Evaluating Impact

Following the approach presented in section 2.1.2, the following analysis can be made:

Loss of confidentiality

Within the scope of the employees’ recruitment operation, as described above, the loss of confidentiality could allow disclosure of data of the candidates, potentially leading to embarrassment or defamation. This is mainly related to the evaluation results, that may provide an assessment of the candidate’s professional experience and capacity, as well as other personal qualities (e.g. ability to communicate well or express himself/herself clearly). For the purpose of this use case, we assume that the recruitment platform provides for a structured assessment of the candidates, based on specific professional criteria, and does not include other types of assessments of the personality or characteristics of the candidate (e.g. psychological profile). Following the aforementioned description, the data subject is expected to encounter from minor to serious inconvenience from loss of confidentiality, which could in some cases influence her ability of getting employed. Therefore, the impact level for this case could in general be considered as MEDIUM.

Loss of integrity

The level of impact resulting from loss of integrity is considered to be MEDIUM as unauthorized alteration of personal data processed could either hinder the successful accomplishment of the recruitment procedure or amend the eligibility/ interview report of a candidate (and, thus, her possibility of getting employed).

Loss of availability

The level of impact resulting from loss of integrity is considered to be LOW as data subjects are expected to encounter minor inconvenience, due to the delay of the process, which will not be invalidated though. The next table summarizes the aforementioned analysis.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**

Overall Impact Evaluation	MEDIUM

The overall result of the evaluation of the impact is the highest identified and therefore the overall impact evaluated is MEDIUM.

Further to the assumptions made in this example, there might be cases where the overall impact could be higher from the one calculated above. For example, such could be the case of an evaluation process including psychological tests or specific behavioural characteristics of the candidates. Another case could be if personal data related to disabilities, ethnic background etc. are also processed.

3.2.3 Threat Occurrence Probability

Based on the questions, presented in Section 2.1.3, we the following assessment was made for each dimension of the processing operations' environment:

- **Network & technical resources:** The threat occurrence probability is LOW as the processing is not performed through the Internet and the evaluation platform is a dedicated system, which is not connected to other IT systems of the SME. Like in previous cases, it is assumed that best practices are deployed to prevent unauthorized access and accordingly safeguard the data.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is LOW, assuming that roles and responsibilities of employees involved are clearly defined along to an acceptable use policy, processing of personal data is limited to the premises of the organization and log files are created for any processing activity.
- **Parties/People involved in the processing of personal data:** The threat occurrence probability is MEDIUM as it includes a large number of employees involved in the processing (HR officers, selection committee, senior management) and it is assumed that not all employees involved in the processing have received relevant information security training.
- **Business sector and scale of processing:** The threat occurrence probability is LOW as the business sector of the SME is in general not considered prone to cyberattacks and no personal data breach is known to have occurred in the past. The processing operation is limited only to the employees of the SME.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	Low	1
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Medium	2
Business sector and scale of processing	Low	1
Overall Threat Occurrence Probability	Low (5)	

Following the aforementioned assessment, the overall threat occurrence probability is calculated as LOW.

3.2.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨 X	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as MEDIUM. Annex A: (A.1 & A.2) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (higher) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability. For example, if the candidates have access to their evaluation reports directly through the recruitment IT platform, the threat occurrence probability would probably be increased to HIGH. See also relevant considerations under section 3.3.2 for impact evaluation.

3.3 Evaluation of employees

Within the scope of this use case, we consider as an example an SME specializing in IT products and relevant consultancy services. On a yearly basis, each employee is evaluated by the line manager against predefined and pre-agreed criteria related to his/her performance and professional characteristics, which include reliability, orientation towards users/customers, timeliness/readiness, interpersonal skills, flexibility, autonomy, written and oral communication skills and team spirit. The processing is performed by an HR officer and line managers with electronic tools and paper documentation. The line manager produces a first version of the report on paper and discusses the findings with the employee. The final version of the report is duly signed and submitted electronically to the HR department while the summary and the conclusions/findings of the report are submitted electronically as well.

3.3.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	EVALUATION OF STAFF	
Personal Data Processed	**First and last name, position within the SME, date of employment, employment history, technical skills, knowledge and behaviours (work performance evaluation reports)**	
Processing Purpose	**Assessment of the performance and professional characteristics that arise in the execution of the work**	
Data Subject	**Employees**	
Processing Means	**Human Resources IT System**	
Recipients of the Data	**Internal**	**Line Managers**
Data Processor Used	**In-house (no data processor)**	

3.3.2 Evaluating Impact

Following the approach presented in section 2.1.2, the following analysis can be made:

Loss of confidentiality

Within the scope of this processing operation, it should be taken into account that the staff assessment provides a detailed professional profile of the employee by attributing quantitative and qualitative values to her performance at work. Although evaluation may be limited to work performance, in the course of the exercise, other individual's characteristics may emerge, creating a marginal risk that information relating to the behavior and personality of the employees is also processed. The loss of confidentiality of this data could range from simple discomfort to dishonor or even limitation of the employee, e.g. when seeking for a new job. Therefore, the impact of loss of confidentiality is considered as MEDIUM.

Loss of integrity

The loss of integrity might be in general considered as MEDIUM as data subjects are expected to encounter significant inconveniences including improper evaluation or lack or delays in benefitting from the results of the evaluation.

Loss of availability

The loss of availability might be in general considered as LOW as data subjects are expected to encounter minor inconveniences due to the delay of the process, which will not be invalidated though. The next table summarizes the aforementioned analysis.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**
	Overall Impact Evaluation	**MEDIUM**

The overall result of the evaluation of the impact is the highest identified and therefore the overall impact evaluated is MEDIUM.

Further to the assumptions made in this example, there might be cases where the overall impact could be higher from the one calculated above. An example of such case could be when the:

- Specific working context requires an assessment of the psychological characteristics of the employees or when sensitive data are included in the course of the evaluation process (e.g. relating to persons with disabilities).

3.3.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources:** The threat occurrence probability is LOW, as the system is not connected to the internet and does not allow access from internet to internal resources and other IT systems. It is assumed for this use case that unauthorized access is prevented based on relevant best practices.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is MEDIUM, assuming that the use policy is not clearly defined and processing of information is not necessarily limited to the premises of the organization (paper based process).

- **Parties/People involved in the processing of personal data:** The threat occurrence probability is MEDIUM as it is assumed (from the case description) that there no specific policies regarding secure storage and deletion of data (especially when part of the process is paper based).
- **Business sector and scale of processing:** The threat occurrence probability is LOW as the business sector of the SME is in general not considered prone to cyberattacks and it is assumed that no personal data breach is known to have occurred in the past. The processing operation is limited only to the employees of the SME.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Low**	**1**
Processes/Procedures related to the processing of personal data	**Medium**	**2**
Parties/People involved in the processing of personal data	**Medium**	**2**
Business sector and scale of processing	**Low**	**1**
Overall Threat Occurrence Probability	**Medium (6)**	

Following the aforementioned assessment, the overall threat occurrence probability is calculated as MEDIUM.

3.3.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨 **X**	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as MEDIUM. Annex A: (A.1 & A.2) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (higher) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 3.3.2).

4. Use cases: Customers management, marketing and suppliers

A typical SME will process personal data of its customers and perform marketing activities so as to attract new customers. It may also process personal data in relation to its suppliers. Depending on the nature of business activities, the nature and amount of products and services portfolio, as well as the target market, the activities may differentiate and include processing of different types of personal data in a different scale or/and for different purposes.

4.1 Order and delivery of goods

Within the scope of this use case, we consider a retail SME that offers goods through a dedicated e-shop. Customers can browse through the available goods, add them to the cart and check out. In order to complete the order, the customer has to register at the e-shop platform (if not already registered) and provide her contact details (first and last name, delivery address, telephone number and email address). During the checkout process, registered users are also asked to provide payment details in a separate form, which is provided by the payment services provider. Following the successful placement of the order and the confirmation from the payment service provider, the details of the order are transmitted to the Enterprise Resource Planning (ERP) system, to the Customer Relation Management (CRM) system and to the delivery services provider. Regarding the use of the system there is a specific use policy in place and best practises are implemented and maintained. However, there are no specific policies regarding data retention and destruction and not all employees involved has received relevant information security training.

4.1.1 Definition of the processing operation and its context

The specific data processing operation can be detailed, as follows:

PROCESSING OPERATION DESCRIPTION	ORDER AND DELIVERY OF GOODS	
Personal Data Processed	**Contact information (last and first name, address, telephone number) payment data (credit card, bank account information)**	
Processing Purpose	**Order and delivery of goods**	
Data Subject	**Customers**	
Processing Means	**Order Management system**	
Recipients of the Data	**External**	**Payment services provider**
	External	**Delivery services provider**
	Internal	**Customer Relation Management (CRM) system**
	Internal	**Enterprise Resource Planning (ERP) system**
Data Processor Used	**In-house and external parties**	

4.1.2 Evaluating Impact

Loss of confidentiality and integrity

Within the scope of the specific processing operation, as described earlier, the impact from loss of confidentiality and/or integrity is considered as MEDIUM, as unauthorized disclosure and/or alteration of personal data processed, including financial data, could result in significant inconveniences for the data subject (which can be recovered with some effort).

Loss of availability

The level of impact resulting from loss of availability is considered to be LOW, as unavailability of the personal data processed is expected to result only to minor inconveniences for the data subject which can easily be overcome, e.g. delay of the delivery of goods.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**
	Overall Impact Evaluation	**MEDIUM**

The overall result of the evaluation of the impact is therefore MEDIUM.

Further to the assumptions made in this example, there might be cases in which the overall impact could be different (higher) from the one calculated above. An example could be the case when goods available for order can reveal sensitive data about the individual, e.g. relating to her health, sexual or political and religious preferences.

4.1.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources:** The threat occurrence probability is MEDIUM, as part of the processing of personal data is performed through the internet and the processing system is interconnected to another internal and external IT systems. It is assumed for this use case that unauthorized access to personal data is prevented based on relevant best practices.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is LOW, as it assumed that roles and responsibilities of employees are clearly defined in line with an acceptable use policy, the processing of personal data is limited to the premises of the organization and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data:** The threat occurrence probability is MEDIUM as not all employees have received relevant information security training and it is not ensured that personal data are always securely processed and/or destroyed.
- **Business sector and scale of processing**: The threat occurrence probability is MEDIUM as the business sector of the as the business sector of the SME (e-shop) can be considered in general as prone to cyberattacks and the processing operation does concern a large number of individuals. However, it is assumed for the particular case that a personal data breach has very occurred in the past.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Medium**	**2**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**Medium**	**2**
Business sector and scale of processing	**Medium**	**2**

Overall Threat Occurrence Probability	**Medium (7)**

Following the aforementioned assessment, the overall threat occurrence probability is calculated as MEDIUM.

4.1.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨 **X**	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as MEDIUM. Annex A (A.1 & A.2) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (higher) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 4.1.2).

4.2 Marketing/advertising

Within the scope of this use case, we consider the retail SME described in section 4.1, which processes personal data of potential customers in order to promote the different kinds of goods available within its portfolio. For such processing to take place it is assumed that data subjects have already provided their consent via paper or electronic form (we do not make any legal analysis in the context of the use case).

For this processing operation, the SME makes use of a dedicated web tool, offered by a third party provider who specializes in such activities. The third party provider is EU based and adheres to relevant security best practices. Each month, an officer from the marketing department, inserts to the web tool, through an appropriate web interface the contact information (first and last name, email address) of potential customers and updates the list with any potential customers that have requested not to be included in the list. Every week, the officer initiates a new marketing campaign through the web tool, which then sends respective personalized emails, to the lastly updated recipients list. For each campaign, the tool provides a report with statistics on the percentage of emails read, unread, deleted without however providing information on specific individuals.

4.2.1 Definition of the processing operation and its context

The specific data processing operation can be detailed, as follows :

PROCESSING OPERATION DESCRIPTION	MARKETING/ADVERTISING
Personal Data Processed	**Contact info (e.g name, postal address, telephone number, email)**

Processing Purpose	**Promotion of goods and special offers to possible customers**	
Data Subject	**Customers and potential Customers**	
Processing Means	**Third party marketing campaign web service**	
Recipients of the Data	**External**	**Third party marketing campaign web service provider**
	Internal	**Marketing Department**
	Internal	**CRM IT system**
Data Processor Used	**Third party marketing campaign web service provider**	

4.2.2 Evaluating Impact

Loss of confidentiality, integrity and availability

Within the scope of the specific operation, the impact from loss of confidentiality, and/or integrity and/or availability is considered to be LOW, as individuals may encounter some minor inconvenience, e.g. by unauthorized disclosure of their contact info (which could lead to spam) or unauthorized modification of their data, excluding them from a potential marketing campaign. In all cases the issue can be easily resolved with some small effort.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Low	**Low**	**Low**
	Overall Impact Evaluation	**LOW**

The overall result of the evaluation of the impact is therefore LOW.

Further to the assumptions made in this example, there might be cases where the overall impact could be different (higher) from the one calculated above. An example could be a case where the inclusion of the individual in a marketing campaign may reveal sensitive information, e.g. related to her racial or ethnic origin, political opinions or health status.

Another example could be if the processing operation included processing of personal data in order to cultivate a better understanding of customers and potential customers' habits, preferences and eventually orient appropriately their marketing strategies. This type of processing would then be characterized as 'profiling' and data related to data subject's possible preferences and interests (acquired through the profiling process). Within the scope of this specific processing operation, the impact from loss of confidentiality would then be considered as MEDIUM, as individuals may encounter in certain cases significant problems by having their preferences, shopping habits, interests being accessed by third parties in an unknown way. It could be raised to HIGH, e.g. in case that this profiling is based on sensitive data.

4.2.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources**: The threat occurrence probability is MEDIUM, as the processing of personal data is performed through the internet and the processing system is interconnected to other internal and external IT systems.

- **Processes/Procedures related to the processing of personal data**: The threat occurrence probability is LOW, as it is assumed that processes are well defined and the specialised third party adheres to security best practices in the field.
- **Parties/People involved in the processing of personal data**: The threat occurrence probability is MEDIUM as part of the data processing operation is performed by a data processor (third party) and, thus, the SME is not in full control of the data. Still, it is assumed that the specialised third adheres to security best practices in the field.
- **Business sector and scale of processing**: The threat occurrence probability is MEDIUM as the business sector of the SME (e-shop) is in general prone to cyberattacks and the processing operation does concern a large number of individuals. However, it is assumed that a personal data breach has never occurred in the past.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Medium**	**2**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**Medium**	**2**
Business sector and scale of processing	**Medium**	**2**
Overall Threat Occurrence Probability	**Medium (7)**	

Following the aforementioned assessment, the overall threat occurrence probability is calculated as MEDIUM.

4.2.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩 **X**	🟨	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is considered as LOW. Annex A (A.1) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (Medium of even High) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 4.2.2).

4.3 Suppliers of services and goods

Within the scope of this use case, we consider the retail SME described in 4.1, which acquires services and goods needed for both day to day operation and also for sale of goods. These procedures may include in certain cases processing of personal data, for instance, contact data of specific employees working for the suppliers or contact and financial data of persons that are in direct contract with the SME (i.e. directly acting as suppliers of goods or services).

The processing operation is supported by an IT system connected to the Enterprise Resource Planning (ERP) system and the Accounting System. The processed personal data include company name and contact details, financial data (tax number, banking account), employee pictures and access credentials (for staff working within premises).

All business relationships between SMEs and suppliers take place using CRM via extranet, directly to the platforms of the suppliers. Payments are made using remote banking services. There is an off-line platform where delivery bills and invoices are loaded overnight in batches. Administrative communications with suppliers take place through ordinary email service.

4.3.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	PROCUREMENT (SUPPLY OF RAW MATERIALS, GOODS AND SERVICES)	
Personal Data Processed	**First and last name, contact Information, tax and banking information (for supplier), picture and access credentials (for staff working on premises).**	
Processing Purpose	**Supply Management**	
Data Subject	**Employees working for suppliers of goods and services**	
Processing Means	**IT system**	
Recipients of the Data	**Internal**	**Enterprise Resource Planning (ERP) system**
	Internal	**Accounting system**
	External	**Suppliers CRM**
	External	**Payment Services Provider**
Data Processor Used	**In-house (no data processor)**	

4.3.2 Evaluating Impact

Loss of confidentiality

Within the scope of the specific processing operation, the impact from loss of confidentiality is considered as LOW, as individuals may encounter in certain cases minor problems by having their processed personal data being accessed by third parties in an unknown way.

Loss of integrity and availability

The impact from loss of integrity and/or availability is considered LOW as individuals may encounter the inconvenience of delaying the accomplishment of the business relationship between the companies, or could divert the ordered goods to an incorrect address or nor delivered at all, but this can be overcome with limited effort.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Low	**Low**	**Low**

Overall Impact Evaluation	LOW

The overall result of the evaluation of the impact is LOW.

Further to the assumptions made in this use case, there might be cases where the overall impact could be different (higher) from the one calculated above. An example of such case could be when the company operates in a 'sensitive' environment and, thus, the disclosure of employees' names might put them at risk (e.g. in a military environment).

4.3.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources**: The threat occurrence probability is MEDIUM, as the system is connected to the internet and it is possible to provide access to the internal personal data processing system through the internet. However, best practices are used to prevent unauthorized access.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is LOW, as it is assumed that roles and responsibilities of personnel are clearly defined along to an acceptable use policy, employees are not allowed to bring their own devices and store, transfer or ortherwise process personal data outside the premises of the organization and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data:** Threat occurrence probability for is LOW as employees are not able to transfer, store or otherwise process personal data outside the premises of the organization while the acceptable use of the network, system and physical resources within the organization is clearly defined and employees involved in the data processing operation securely store and destroy personal data.
- **Business sector and scale of processing:** The threat occurrence probability is LOW as the business sector of the SME is in general not considered prone to cyberattacks, a security breach incident or a complaint has not been received during the last two years and the processing operation does not concern a large number of individuals.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	Medium	2
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Low	1
Overall Threat Occurrence Probability	Low (5)	

4.3.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩 X	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as LOW. Annex A (A.1) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (Medium of even High) under conditions directly related to the specific data processing operation (see also relevant considerations under section 4.3.2).

5. Safety and security

5.1 Access control

Within the scope of this use case, we consider as an example a consulting company (SME) that processes the personal data of its employees and visitors for physical access control within its premises, in order to ensure that only the authorized individuals have access into and out of specific areas.

The deployed access control system comprises of RFID card readers installed in predefined points, RFID cards and the access control management platform. Each employee, upon taking up his or her duties, is registered to the access control management platform and is assigned a unique alphanumeric value which is stored in an RFID card. The personal data used during the registration include first and last name, date of employment, position within the organization, end of employment (if specified by the contract) and a profile picture. Each employee's RFID card is personalized as the name of the employee and his/her profile picture are printed on the card. For each type of position within the organization (administration, manager, secretariat support etc.) specific access rights are predefined. Each time an employee swipes her card against a reader, the platform checks the rights and grants access to the premise accordingly. Each attempt is logged within the platform and in case of an unauthorized access attempt, the security officer is notified. Visitors are also issued respective anonymized visitor RFID cards which are preset to allow access only to meeting rooms. Upon arrival of a visitor, the security officer registers within the platform the first and last name of the visitor, the accompanying employee's first and last name and the expected duration of the visit and assigns temporarily a RFID card to the visitor. Upon departure or expiry of the duration of visit, the card is invalidated and is returned to the security officer. Security officers operating the platform have received special training on the functions of the platform and their obligations and it is assumed that best practices are followed.

PROCESSING OPERATION DESCRIPTION	ACCESS CONTROL	
Personal Data Processed	**For employees: first and last name, date of employment, position within the organization, end of employment, a profile picture.** **For visitors: first and last name, date and time of visit, expected time of departure.**	
Processing Purpose	**Physical-logical Access Control Security**	
Data Subject	**Employees, visitors**	
Processing Means	**Access control management platform**	
Recipients of the Data	**Internal**	**Security Officer**
Data Processor Used	**In-house (no data processor)**	

5.1.1 Evaluating Impact

Loss of confidentiality, integrity and availability

Within the scope of the specific processing operation, the impact from loss of confidentiality, and/or integrity and/or availability is considered to be LOW as individuals are expected to encounter minor inconveniences which they will be able to overcome with limited effort. For example, employees might not be able to access specific premises of the SME and perform their task (integrity or availability loss) or a visitor's presence in the SME premises might be disclosed (confidentiality loss).

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Low	**Low**	**Low**
	Overall Impact Evaluation	**LOW**

The overall result of the evaluation of the impact is therefore LOW.

Further to the assumptions made in this example, there might be cases where the overall impact could be different (higher) from the one calculated above. An example of such case is when the visit to the SME's premises may reveal specific sensitive information, e.g. with regard to health, religious beliefs, political or sexual preferences.

5.1.2 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources**: The threat occurrence probability is LOW, as the system is not connected to the internet, it does not allow access from internet to internal resources and connection to other IT systems and it is assumed that best practices are used to prevent unauthorized access to the system.
- **Processes/Procedures related to the processing of personal data**: The threat occurrence probability is LOW, as it is assumed that roles and responsibilities of security officer are clearly defined along to an acceptable use policy and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data:** The threat occurrence probability is LOW as the security officer is not able to transfer, store or otherwise process personal data outside the premises of the organization while the acceptable use of the network, system and physical resources within the SME is clearly defined.
- **Business sector and scale of processing:** The threat occurrence probability is LOW as the business sector of the SME is not in general considered prone to cyberattacks, a personal data breach has not occurred in the past and the processing operation does not concern a large number of individuals.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Low**	**1**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**Low**	**1**
Business sector and scale of processing	**Low**	**1**
Overall Threat Occurrence Probability	**Low (4)**	

5.1.3 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩 X	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as LOW. Annex A (A.1) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (Medium or even High) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 5.1.2). For example, the threat occurrence probability might be higher in case where the SME operates in a 'sensitive' environment, e.g. a health data laboratory (thus, increasing the possibilities of malicious attempts to gain unauthorised access to premises).

Moreover, account should be taken in general to the fact that access control is an integral measure for preventing unauthorised access to one's premises and, thus, directly linked to security and safety of persons and goods. Therefore, depending again on the nature of the organisation, the SME might consider increasing the overall risk to MEDIUM or even HIGH.

5.2 Closed Circuit Television System (CCTV)

Within the scope of this use case, we consider the SME described in section 5.1, which also processes personal data by means of CCTV (images and video with no sound), in order to enhance the security and safety of people and goods in their premises. It should be noted that the use case does not aim at making any legal analysis or on the use of CCTV; we, therefore, assume that the processing is GDPR compliant and that the guidance of the Data Protection Authority (DPA) has been taken into account. Still, we note that in all cases special attention should be paid to the legal basis of CCTV operation, which should be in compliance with both data protection and labour legal and normative requirements and obligations.

The CCTV system in our example comprises of the camera, and the CCTV management IT system which records the feed, displays it to the security officers and logs any activity on processing non –real time feeds. The feed is stored for the time indicated by the DPA and is then automatically deleted securely, unless the operator extracts it manually for cases which require further examination (for example a security alarm during non-working hours, etc.) Security officers operating the platform have received special training on the functions of the platform and their obligations and it is assumed that best practises are used to avoid authorized access to the feed.

Special attention should be paid to the legal basis of the installation and operation of the CCTV system, which should be in compliance to both data protection and labour legal and normative requirements and obligations.

5.2.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	CCTV
Personal Data Processed	Image and video of persons (employees, visitors).
Processing Purpose	Physical Security of personnel, visitor and goods
Data Subject	Employees, visitors
Processing Means	CCTV IT system
Recipients of the Data	Internal
Data Processor Used	In-house (no data processor)

5.2.2 Evaluating Impact

Loss of confidentiality

Within the scope of the specific processing operation, the impact from loss of confidentiality is considered to be LOW as individuals might in certain cases encounter minor inconvenience or discomfort, for example if the presence of a visitor in the SMEs premises is unwantedly revealed.

Loss of integrity and availability

The loss of integrity is rather hard to achieve (from a technical point of view) in this particular case, as it would require manipulation of the video images. Loss of availability relates to the unavailability (full or temporal) of video footage. In both cases, the impact is considered LOW and it could even be stated that there is no impact for the individuals at all (as loss of CCTV footage is a problem for the SME, but not for the individuals who are being recorded).

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Low	**Low**	**Low**
	Overall Impact Evaluation	**LOW**

The overall result of the evaluation of the impact is therefore LOW.

Further to the assumptions made in this example, there might be cases where the overall impact could be different (higher) from the one calculated above. An example of such case is when the visit to the SME's premises could reveal or infer sensitive information, e.g. related to health status, religious beliefs, political or sexual preferences.

5.2.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources:** The threat occurrence probability is LOW, as the system is assumed to not be connected to the internet and best practices are used to prevent unauthorized access.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is LOW, as roles and responsibilities of security officers are clearly defined along to an acceptable use policy and log files are created for any processing activity being performed

- **Parties/People involved in the processing of personal data:** The threat occurrence probability is LOW as employees are not able to transfer, store or otherwise process CCTV data outside the premises of the organization while the acceptable use of the network, system and physical resources within the organization is clearly defined.
- **Business sector and scale of processing:** The threat occurrence probability is LOW as the business sector of the SME is not in general considered as prone to cyberattacks and, a personal data breach has not occurred in the past. Moreover, the processing operation does concern a large number of individuals.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	Low	1
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Low	1
Overall Threat Occurrence Probability	Low (4)	

5.2.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩 X	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as LOW. Annex A (A.1) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (Medium or even High) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 5.2.2). For example, the threat occurrence probability might be higher in case where the SME uses advanced CCTV systems, which allow zooming and video recording (note that in such cases the overall legality of the data processing operation should be carefully analysed).

6. Specific use case: Health sector

6.1 Health Services Provision

Within the scope of this use case, we consider an SME in the health care domain (small clinic) which processes personal data in order to provide healthcare services. For each patient visiting the clinic to perform an examination or a consultation visit, an electronic record is created (or updated) and includes patients' contact details, social insurance number, medical exams' results, pathologies, allergies, diagnosis and cure schemas (medical information). Through this record, treating doctors and nurses have an overview of the history and the status of the patients' health and can access it if needed from pre-defined terminals within the clinic premises. Prior to the medical examination or consultation visit, the eligibility of the patient to receive such examination or treatment without covering its cost is validated against the public health system records. If the patient or exanimation is not eligible, the cost is communicated to the accounting IT system which issues the respective invoice. After each examination or consultation visit, patient records are updated with the latest data by the treating doctor or nurse either by scanning paper based documents or inserting manually diagnosis and cure schemas.

The IT platform supporting this processing operation, is hosted within the premises of the SME and it is not accessible through the Internet. For the purpose of the use case, it is assumed that best practises are used to prevent unauthorized access to the platform and that periodical security awareness raising trainings are being organized. Still, access rights to the patients' medical records are not explicitly defined at a granular level, as nurses and doctors need to be able to access the files at any time and the system does not support relevant granularity. The SME plans to have a more dedicated patient record system within the next years.

6.1.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	HEALTH SERVICES PROVISION	
Personal Data Processed	**Contact Information (last and first name, address, telephone number,) social insurance number, medical examination results, pathologies, allergies, diagnosis and cure schemas (medical information), administrative and financial information (invoices, hospitalisation papers, etc.).**	
Processing Purpose	**Provision of healthcare services (diagnosis, treatment an hospitalisation)**	
Data Subject	**Patients**	
Processing Means	**Medical IT system**	
Recipients of the Data	**Internal**	**Treating doctors and nurses**
	Internal	**Administration and accounting IT system**
	External	**Public Health System**
Data Processor Used	**In-house (no data processor)**	

6.1.2 Evaluating Impact

Loss of confidentiality, integrity and availability

Within the scope of the specific processing operation, the impact from loss of confidentiality is considered to be HIGH as individuals are expected to encounter major adverse effects through unauthorized access to their health related data. Equally important (HIGH) may be the loss of integrity, as wrong medical information might even put an individual's life at risk. The same (HIGH) could be argued also for the loss of availability, as even a temporal unavailability of the clinic's IT system might hinder its operations, thus putting patients at serious risk.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
High	**High**	**High**
	Overall Impact Evaluation	**HIGH**

The overall result of the evaluation of the impact is therefore HIGH.

Further to the assumptions made in this example, there might be cases where the overall impact could even be considered as VERY HIGH, for example in cases of vulnerable categories of data subjects or minors.

6.1.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources:** The threat occurrence probability is MEDIUM, as the system is interconnected to other external and internal systems. However, the data cannot be accessed via the Internet and, according to the use case description, security best practices have been applied to prevent unauthorized access to the system.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is LOW, as roles and responsibilities of personnel are clearly defined along to an acceptable use policy, the processing of data is limited in the premises of the SME and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data:** The threat occurrence probability is HIGH as processing of personal data is performed by an undefined number of employees and there is no clear policy regarding granular access to the health records. However, the obligations of all parties involved in the processing are clearly defined and awareness raising seminars are organized periodically.
- **Business sector and scale of processing**: The threat occurrence probability is HIGH as the business sector of the SME (healthcare) is in generally considered prone to cyberattacks and the processing operation does concern a large number of individuals. However, it is assumed that as personal data breach has not occurred in the past.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Medium**	**2**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**High**	**3**
Business sector and scale of processing	**High**	**3**
Overall Threat Occurrence Probability	**HIGH (9)**	

6.1.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥 X

In particular, the overall risk for this particular case is generally considered as HIGH. Annex A (A.1 & A.2 & A.3) can be used for the adoption of measures appropriate to the risk presented.

6.2 Medically Assisted Procreation

Within the scope of this use case, we consider an SME in the health care domain specializing in Medically Assisted Procreation (MAP) that processes personal data for management and tracking of biological samples stored within its premises. MAP includes different methods or techniques based on the manipulation of reproductive cells that will allow infertile couples to conceive a child. MAP procedures also include cryopreservation techniques for gametes (oocytes and spermatozoa) and embryos.

The IT system deployed internally to support MAP holds records for each sample that include: information of the donor (first and last name, address, telephone number, date of birth), social insurance number, health data, genetic sample data and genetic sample identifier. Through the platform, the operator can perform the following functions: a) sample management, traceability of all sample manifestations, sample position management within cryogenic containers, and b) access management and registration of cryopreserved samples.

Regarding the use of the IT system, a specific use policy is in place alongside specific policies regarding data retention and destruction. Processing of personal data is limited to the premises of the SME. Access to the platform is allowed only to specific employees of the SME, acting as the operators, and to the doctor and biologist employees responsible for performing MAP. All platform users have been clearly informed about their obligations regarding personal data processing and awareness-raising training is organized periodically. The platform is not connected to the internet and it is assumed that best practises are used to prevent unauthorised access.

6.2.1 Definition of the processing operation and its context

The specific data processing operation can be detailed, as follows:

PROCESSING OPERATION DESCRIPTION	MANAGEMENT OF BIOLOGICAL SAMPLES FOR MEDICALLY ASSISTED PROCREATION
Personal Data Processed	**Information of the donor (first and last name, address, telephone number, date of birth), social insurance number, health data, genetic sample data and genetic sample identifier**
Processing Purpose	**Management of genetic sampled for Medically Assisted Procreation (MAP)**
Data Subject	**Donors**

PROCESSING OPERATION DESCRIPTION	MANAGEMENT OF BIOLOGICAL SAMPLES FOR MEDICALLY ASSISTED PROCREATION	
Processing Means	**Medically Assisted Procreation Management IT system**	
Recipients of the Data	**Internal**	
Data Processor Used	**In-house (no data processor)**	

6.2.2 Evaluating Impact

Following the approach presented in section 2.1.2, the following analysis can be made:

Loss of confidentiality, integrity and availability

Within the scope of the specific processing operation the impact from loss of confidentiality is considered HIGH, as data subjects are expected to encounter significant adverse effects from unauthorised disclosure of health and genetic data. The impact from loss of integrity or availability is equally important (HIGH), as data subjects are expected to encounter significant or even irreversible inconvenience from unauthorised alteration or loss of health and genetic data, which could even prevent them from undergoing a MAP procedure.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
High	**High**	**High**
	Overall Impact Evaluation	**HIGH**

The overall result of the evaluation of the impact is the highest identified and therefore the overall impact evaluated is HIGH

Further to the assumptions made in this example, there might be cases where the overall impact could be even be considered as VERY HIGH, for example, in cases of vulnerable categories of data subjects (e.g. data subjects with specific diseases or handicaps)

6.2.3 Threat Occurrence Probability

- **Network & technical resources**: The threat occurrence probability is LOW, as the system is not connected to the internet, it is not possible to provide access to the internal personal data processing system through the internet and best practices are used to prevent unauthorized access.
- **Processes/Procedures related to the processing of personal data**: The threat occurrence probability is LOW, as roles and responsibilities of personnel are clearly defined along to an acceptable use policy, the processing is limited to the premises of the SME and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data**: The threat occurrence probability is LOW as processing of personal data is performed by a defined number of employees with clearly defined obligations and it is assumed that employees involved in the data processing operation securely store and destroy personal data.
- **Business sector and scale of processing**: The threat occurrence probability is HIGH as the business sector of the SME could be considered as prone to cyberattacks and could potentially concern a large number of individuals. However, it is assumed that no personal data breach is known to have occurred in the past.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Low**	**1**
Processes/Procedures related to the processing of personal data	**Low**	**1**
Parties/People involved in the processing of personal data	**Low**	**1**
Business sector and scale of processing	**High**	**3**
Overall Threat Occurrence Probability	**Medium (6)**	

6.2.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥 X
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as HIGH. Annex A (A.1 & A.2 & A.3) can be used for the adoption of measures appropriate to the risk presented.

6.3 Remote monitoring of patients with chronic diseases

Within the scope of this use case, we consider an SME in the health care domain specializing in providing homecare remote monitoring services for patients who have been diagnosed with a chronic condition. Each patient is provided with a monitoring device, which allows real time tracking of vital signs and transmission of information such as blood pressure, glucose level, pulse and ECG rhythm in set intervals diagnoses to the affiliated healthcare centre. The monitoring device also acts as a communication device, enabling patients to respond to personalized clinician-directed surveys related to the compliance level of treatment schemas.

The remote monitoring device is supported by a web-based platform, hosted by a cloud provider within the EU, which collects and correlates all data transmitted in order to detect any deviations from the clinical protocol and determine the overall health status of the patient. Should a deviation from acceptable values and procedures is detected, a medical practitioner communicates through phone with the patient to determine whether an in house visit is required.

The personal data involved in the processing operation include patients' personal information, such as first and last name, address, telephone numbers, date of birth, alongside social insurance number, health status data, diagnosis results, treatment schemas, vital signs readings and relevant statistics. The web platform is operated by authorized medical practitioners with clearly defined roles, responsibilities and obligations related to personal data processing.

6.3.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	REMOTE MONITORING OF PATIENTS WITH CHRONIC DISEASES	
Personal Data Processed	**First and last name, address, telephone numbers, date of birth, social insurance number, health status data, diagnosis results, treatment schemas, laboratory test results and relevant statistics.**	
Processing Purpose	**Healthcare service provision (remote monitoring of patients with chronic diseases_**	
Data Subject	**Patients**	
Processing Means	**Remote Monitoring devices, Monitoring web-based platform**	
Recipients of the Data	**External**	
	Internal	
Data Processor Used	**Hosting cloud provider**	

6.3.2 Evaluating Impact

Loss of confidentiality, integrity and availability

Within the scope of the specific processing operation, the impact from loss of confidentiality is considered HIGH as data subjects are expected to encounter significant adverse effects from unauthorised disclosure of their health data. The loss of integrity is equally important (HIGH), as data subjects are expected to encounter significant or even irreversible inconvenience from unauthorised alteration of health data (signals and statistics), which could even make it difficult for them to receive appropriate treatment. The loss of availability is also HIGH, as it could again hinder the timely and accurate treatment of the data subjects, which could even put their lives at risk.

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
High	**High**	**High**
	Overall Impact Evaluation	**HIGH**

The overall result of the evaluation of the impact is the highest identified and therefore the overall impact evaluated is HIGH.

Further to the assumptions made in this example, there might be cases where the overall impact could even be considered as VERY HIGH, for example, when the processing relates to minors.

6.3.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources**: The threat occurrence probability is HIGH, as the system is connected to the internet and it is possible to provide access to the internal personal data processing system through the internet. Moreover, different tools and systems are interconnected and many different systems need to be equally secured.

- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is MEDIUM, as roles and responsibilities are complex in this scenario, due to many different actors and systems involved.
- **Parties/People involved in the processing of personal data:** The threat occurrence probability is HIGH as a data processor is used, which is based on the cloud. Still, the processing is performed by a pre-defined number of employees and it is assumed that they receive periodic awareness raising trainings.
- **Business sector and scale of processing:** The threat occurrence probability is HIGH as the business sector of the SME could be considered as prone to cyberattacks and could potentially concern a large number of individuals. However, it is assumed that no personal data breach is known to have occurred in the past.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	High	3
Processes/Procedures related to the processing of personal data	Medium	2
Parties/People involved in the processing of personal data	High	3
Business sector and scale of processing	High	3
Overall Threat Occurrence Probability	High (11)	

6.3.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨	🟥
	High	🟨	🟥	🟥 X

In particular, the overall risk for this particular case is generally considered as HIGH. Annex A (A.1 & A.2 & A.3 can be used for the adoption of measures appropriate to the risk presented.

7. Specific use case: Education sector

7.1 Early childhood – Crèche

Within the scope of this use case, we consider an early childhood school which uses a web platform to support communication of day to day physical, intellectual, language, emotional and social activities of minors between the school and the parents. In addition, the platform may also include information on the childrens' health, appetite and disposition (provided by the parents). Parents are also able to communicate with the educator and seek advice and support on how to nurture and better support the cognitive and social-emotional development of their infant.

The platform is hosted at an EU based hosting provider and operated by the educators. Each educator manages and updates information about the children assigned to his or her classroom, while the overall administration of the platform is performed by the secretariat of the school. Parents are registered to the platform by the secretariat and can only access and update the data of their child. It is assumed that best practices are being used to prevent unauthorized access, roles and responsibilities of employees involved are clearly defined and communicated, and log files are created for all data processing activities. The platform processes the following data: first and last name, date of birth, home address, daily information on the child's performance (including eating, activities, etc.), health data, allergies, nutrition intolerances, parent(s) first and last name, parent(s) telephone number, emergency contact number.

7.1.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	EARLY CHILDHOOD SCHOOL COMMUNICATION PLATFORM	
Personal Data Processed	**First and last name, date of birth, home address, daily information on the child's performance (including eating, activities, etc.), health data, allergies, nutrition intolerances, parent(s) first and last name, parent(s) telephone number, emergency contact number**	
Processing Purpose	**Provision of educational services (communication of day to day activities and child's development)**	
Data Subject	**Children and parents**	
Processing Means	**Web based**	
Recipients of the Data	**External**	**Parents**
	Internal	**Secretariat, Educators**
Data Processor Used	**Web hosting provider**	

7.1.2 Evaluating Impact

Loss of confidentiality

Within the scope of the specific processing operation, the impact from loss of confidentiality is considered as MEDIUM, as in certain cases individuals (children and parents) may encounter significant inconvenience from the disclosure of certain data (e.g. regarding the child's behavior or communication or eating patterns).

Loss of integrity

The loss of integrity can also be considered as MEDIUM, as unauthorized modification of this data could possibly hinder the appropriate provision of services by the crèche (especially with regard to allergies, nutrition patterns and other related data).

Loss of availability

The loss of availability can be considered as LOW, since the unavailability of the data can lead to some minor inconvenience that can be easily overcome (e.g. by entering again the data in the platform or communicating with the parents through other means)..

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**
	Overall Impact Evaluation	**MEDIUM**

The overall result of the evaluation of the impact is the highest identified and therefore the overall impact evaluated is MEDIUM**.**

Further to the assumptions made in this example, there might be cases where the overall impact could be higher than the one calculated above. An example of such case is when there are particular diet plans followed by specific children (e.g. due to religious beliefs). Another example is the case of a school specifically dedicated to children with special conditions or disabilities.

7.1.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources**: The threat occurrence probability is MEDIUM, as the system is connected to the internet and it is possible to provide access to the internal personal data processing system through the internet. However, best practices are used to prevent unauthorized access and it is assumed that these are up-to-date.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is MEDIUM, as there are different parties accessing the same platform and it is not clear if roles and responsibilities have been clearly defined. Still, there is an acceptable use policy in place and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data**: The threat occurrence probability is MEDIUM as a third party data processor is being used and employees are able to transfer, store or otherwise process personal data outside the premises of the school. However, it is assumed that acceptable use of the network, system and physical resources is clearly defined.
- **Business sector and scale of processing**: The threat occurrence probability is LOW as the business sector of the SME (education) is not in general considered as prone to cyberattacks and the processing operation does not concern a large number of individuals. It is assumed that no personal data breach has even occurred in the past.

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Medium**	**2**
Processes/Procedures related to the processing of personal data	**Medium**	**2**
Parties/People involved in the processing of personal data	**Medium**	**2**
Business sector and scale of processing	**Low**	**1**
Overall Threat Occurrence Probability	**Medium (7)**	

7.1.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

		IMPACT LEVEL		
		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨 **X**	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as MEDIUM. Annex A (A.1& A.2) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (higher) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 7.1.2).

7.2 University e-learning platform

Within the scope of this use case we consider a university which offers an e-learning and course management platform hosted internally in a web server. Through the platform, professors and administration can send announcements to students and students can retrieve their course materials, lecture notes and slides, submit assignments, undertake assessments and tests and get evaluation results and grades. At the beginning of each semester the University's administration department enrols students to modules (courses) and assigns respective privileges to both students and academic staff. It is assumed that best practices are being used to prevent unauthorized access, roles and responsibilities of employees involved are clearly defined and communicated, and log files are created for all data processing activities. For evaluation results, professors submit the final scores to administration in paper, and administration encodes them to the platform. The platform processes the following data: a) Students: first and last name, date of birth, date of admission, selected course(s), evaluation results, grades; b) Academic Staff: first and last name, date of birth, course(s) assigned.

7.2.1 Definition of the processing operation and its context

PROCESSING OPERATION DESCRIPTION	UNIVERSITY'S E-LEARNING PLATFORM	
Personal Data Processed	Students: first and last name, date of birth, date of admission, selected course(s), evaluation results, grades; Academic Staff: first and last name, date of birth, course(s) assigned	
Processing Purpose	e-Learning and course management platform, including undertaking of assignments and test	
Data Subject	Students, Professors	
Processing Means	e-Learning and course management platform	
Recipients of the Data	Internal	University administration
	Internal	Head of Departments
Data Processor Used	In-house (no data processor)	

7.2.2 Evaluating Impact

Loss of confidentiality

Within the scope of the specific processing operation, the impact from loss of confidentiality is considered as MEDIUM, as data subjects are expected to encounter significant inconvenience from unauthorised disclosure of personal data relating their academic performance, grades and results.

Loss of integrity

The impact from loss of confidentiality is considered also as MEDIUM, since data subjects are expected to encounter significant inconvenience from unauthorised alteration of personal data which directly influence their performance and grades.

Loss of availability

The impact from loss of confidentiality is considered LOW, as data subjects are expected to encounter minor inconvenience from unavailability of personal data, which can be easily overcome (assuming that there are back-ups and information on evaluation results and grades is also stored offline).

IMPACT ASSESSMENT		
Confidentiality	Integrity	Availability
Medium	**Medium**	**Low**
	Overall Impact Evaluation	**MEDIUM**

The overall result of the evaluation of the impact is the highest identified and therefore the overall impact evaluated is MEDIUM.

Further to the assumptions made in this example, there might be cases where the overall impact could be different (higher) than the one calculated above. An example of such case could be the possible integration of the platform with social network profiles, where other data are also collected about the students (e.g. lifestyle, habits, etc.). Another example could be the possible use of the platform for statistics and analytics. Note should be taken that in both of these cases, the overall legality of the data processing operations should be carefully assessed.

7.2.3 Threat Occurrence Probability

Based on the questions and approach presented in Section 2.1.3, the following assessment can be made for each dimension of the specific data processing environment of this use case:

- **Network & technical resources**: The threat occurrence probability is MEDIUM, as the system is connected to the internet and it is possible to provide access to the internal personal data processing system through the internet. However, it is assumed that best practices are used to prevent unauthorized access and that these are up-to-date.
- **Processes/Procedures related to the processing of personal data:** The threat occurrence probability is MEDIUM, due to the different parties accessing the system and the fact that roles and responsibilities need to be very clearly set. Still, it is assumed that there is a specific acceptable use policy and log files are created for any processing activity being performed.
- **Parties/People involved in the processing of personal data**: The threat occurrence probability is LOW as a third party data processor is being used and. However, it is assumed that acceptable use of the network, system and physical resources is clearly defined and employees are able to transfer, store or otherwise process personal data outside the premises of the school.
- **Business sector and scale of processing**: The threat occurrence probability is MEDIUM as the processing operation does concern a large number of individuals and the business sector of the SME (higher education - university) could potentially be prone to cyberattacks. It is assumed that no personal data breach is known to have occurred in the past

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
Network and Technical Resources	**Medium**	**2**
Processes/Procedures related to the processing of personal data	**Medium**	**2**
Parties/People involved in the processing of personal data	**Low**	**1**
Business sector and scale of processing	**Medium**	**1**
Overall Threat Occurrence Probability	**Medium (7)**	

7.2.4 Evaluation of Risk

Using the results from impact assessment and threat occurrence probability, the risk is calculated based on Section 2.1.4.

IMPACT LEVEL

		Low	Medium	High / Very High
THREAT OCCURRENCE PROBABILITY	Low	🟩	🟨	🟥
	Medium	🟩	🟨 **X**	🟥
	High	🟨	🟥	🟥

In particular, the overall risk for this particular case is generally considered as MEDIUM. Annex A (A.1 & A.2) can be used for the adoption of measures appropriate to the risk presented.

Note should be taken that the risk might be different (higher) under conditions directly related to the specific data processing operation and affecting either the impact or the threat occurrence probability (see also relevant considerations under section 7.2.2).

8. Conclusions

Security of personal data processing is already a legal obligation for data controllers, however the imminent General Data Protection Regulation reinforces the relevant provisions (both in substance and context) and extends this responsibility directly also to data processors. 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 the ENISA's 2016 guidelines for SMEs[3] (on the security of personal data processing) and provides a practical demonstration of the aforementioned steps through specific use cases. Each use case corresponds to a specific personal data processing operation and makes specific assumptions on the data processing environment and overall context of processing. The provided examples focus only on security measures and do not aim at providing any legal analysis or assessment of compliance with GDPR for the specific data processing operations.

While performing the analysis of selected use cases, a number of conclusions and relevant recommendations were drawn and are discussed below.

Guidance Needed

Similar personal data processing operations may differ among data controllers, taking into consideration their specificities, the means used for the processing of personal data, the categories of data subjects, the data processors and the recipients of data. Therefore, a one-size fits all approach on the overall risk based approach, which extends beyond the data security provisions, cannot be regarded as viable and pragmatic. Each processing operation should be reviewed separately taking also into account the context and environment of the processing. Therefore, instead of a priori categorizing processing operations into risk levels, the focus should be shifted on empowering and guiding the data controllers to first comprehend their processing operations and then evaluate the level of risk and deploy the appropriate security measures.

Competent EU bodies, EU policy makers and regulators (e.g. Data Protection Authorities) should develop practical and scalable guidelines that will be able to support and assist different types of data controllers and address specific stakeholders' communities.

Skilled DPO's

The empowerment of data controllers can also be perceived as a matter of raising their awareness to their processing operations and the overall GDPR provisions. In order, though, to be able to manage their compliance in a more structured manner, rather than a sporadic remedial action, it is expected that they will seek support and guidance. The role of an appropriately qualified Data Protection Officer (DPO) is central in this approach, even when the designation of a DPO is not mandatory according to GDPR Article 37. Having said that, it is important to note that the fulfilment of this role requires both a good understanding of the data protection legal framework, as well as the modern IT technologies (and relevant security best practices), which form the basis for most common data processing means today[9].

[9] See relevant guidelines on Data Protection Officers issued by Article 29 Data Protection Working Party, http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

Competent EU bodies, EU policy makers and regulators (e.g. Data Protection Authorities) should promulgate a set of baseline professional skills and requirements that Data Protection Officers' should meet.

Demonstrating Compliance

As discussed earlier, the security of personal data processing should not be regarded by data controllers as an isolated obligation under GDPR but as part of the overall compliance framework they should develop, implement and maintain. The ENISA methodology can be useful in this regard in all cases where risk assessment is envisaged under the Regulation (e.g. personal data breach notification). Throughout the development of the aforementioned compliance framework, data controllers should try to extend the documentation of their approach, beyond the level imposed by GDPR provisions. This not only ensures that they actively and positively consider the risks of any data processing they undertake but will also step up their efforts with regards to the accountability principle and demonstrating compliance. Furthermore, as the risk based approach is integral part of Data Protection Impact Assessment (DPIA), it is expected that availability of documentation will also facilitate the undertaking, even on a voluntary basis, of the DPIA.

SMEs communities/associations and data controllers should engage in the notion of risk assessment and relevant structured documentation as an integral part of information management systems for personal data.

Regulators (e.g. Data Protection Authorities) should provide guidance and support training for data controllers in this context.

Scalable Certification Schemes

The data protection certification mechanisms of GDPR (Articles 42 and 43) have the potential to play a significant role in enabling data controllers to achieve and demonstrate the existence of appropriate safeguards, including security measures, and therefore compliance of their processing operations with GDPR provisions. As data controllers, and especially SMEs, are relying more and more on third party technologies, products and services, it is important to be encouraged and motivated to assess the level of conformity of these parties and, if possible, acquire such certifications. Given the voluntary nature of certification mechanisms under GDPR, it is crucial that data controllers are motivated and encouraged to adhere to certification schemes, as well as opt for data processors that are following similar practices.

EU policy makers and regulators (e.g. Data Protection Authorities) should define and promote scalable data protection certification schemes, that meet the needs of SMEs and empower them to achieve and demonstrate compliance.

SME communities/associations and data controllers should opt for data processors that adhere to security best practices and relevant certification mechanisms.

Novel Risk Management Methodologies

Information security risk management and risk management of personal data security regard the calculation of risk levels from two different standpoints: the first one focuses on the impact for the data controller and the latter on the impact for data subjects. However, both approaches result in proposed sets of organizational and technical measures to be implemented, maintained and reviewed by the data controller. Regardless of the specificities described earlier, a common methodology, embracing both aspects, could enable data controllers, specifically SMEs, to follow a systematic approach towards reaching compliance.

The research community and competent EU bodies, in close collaboration with regulators (e.g. Data Protection Authorities), should propose and put forward methodologies that combine security risk management and risk management of personal data.

Communication and Awareness Raising

EU SMEs are only starting to consider the changes they should undertake and broaden the perspective of their existing information security and business strategies in order to meet the legal requirements. However, the extent of change(s) required, in order to integrate them into existing business processes, cannot be foreseen. Data controllers are often reluctant and perceive such changes as a barrier rather than an opportunity to position themselves in a newly created market, reinforcing also their customers' confidence and trust.

SME communities and associations, in close collaboration with competent EU bodies and regulators (e.g. Data Protection Authorities), should communicate and encourage data controllers to undertake actions towards security and privacy compliance as a competitive advantage alongside the underlying legal obligations.

Annex A: Organizational and Technical Measures

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

A.1 Proposed Measures for Low Risk Level

🟩	MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
🟩	Security policy and procedures for the protection of personal data	**A.1**	The organization should document its policy with regards to personal data processing as part of its information security policy.	**A.5 Security policy**
🟩	Security policy and procedures for the protection of personal data	**A.2**	The security policy should be reviewed and revised, if necessary, on an annual basis.	**A.5 Security policy**
🟩	Roles and responsibilities	**B.1**	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	**A.6.1.1 Information security roles and responsibilities**
🟩	Roles and responsibilities	**B.2**	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	**A.6.1.1 Information security roles and responsibilities**
🟩	Access control policy	**C.1**	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.	**A.9.1.1 Access control policy**
🟩	Resource/asset management	**D.1**	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).	**A.8 Asset management**
🟩	Resource/asset management	**D.2**	IT resources should be reviewed and updated on regular basis.	**A.8 Asset management**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Change management	**E.1**	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.	**A. 12.1 Operational procedures and responsibilities**
Change management	**E.2**	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.	**A. 12.1 Operational procedures and responsibilities**
Data processors	**F.1**	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.	**A.15 Supplier relationships**
Data processors	**F.2**	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.	**A.15 Supplier relationships**
Data processors	**F.3**	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.	**A.15 Supplier relationships**
Incidents handling / Personal data breaches	**G.1**	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.	**A.16 Information security incident management**
Incidents handling / Personal data breaches	**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.	**A.16 Information security incident management**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Business continuity	**H.1**	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).	**A. 17 Information security aspects of business continuity management**
Confidentiality of personnel	**I.1**	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.	**A.7 Human resource security**
Training	**J.1**	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	**A.7.2.2 Information security awareness, education and training**
Access control and authentication	**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.	**A.9 Access control**
Access control and authentication	**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.	**A.9 Access control**
Access control and authentication	**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.	**A.9 Access control**
Access control and authentication	**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.	**A.9 Access control**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Logging and monitoring	**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).	**A.12.4 Logging and monitoring**
Logging and monitoring	**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	**A.12.4 Logging and monitoring**
Server/Database security	**M.1**	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	**A. 12 Operations security**
Server/Database security	**M.2**	Database and applications servers should only process the personal data that are actually neededs to process in order to achieve its processing purposes.	**A. 12 Operations security**
Workstation security	**N.1**	Users should not be able to deactivate or bypass security settings.	**A. 14.1 Security requirements of information systems**
Workstation security	**N.2**	Anti-virus applications and detection signatures should be configured on a weekly basis.	**A. 14.1 Security requirements of information systems**
Workstation security	**N.3**	Users should not have privileges to install or deactivate unauthorized software applications.	**A. 14.1 Security requirements of information systems**
Workstation security	**N.4**	The system should have session time-outs when the user has not been active for a certain time period.	**A. 14.1 Security requirements of information systems**
Workstation security	**N.5**	Critical security updates released by the operating system developer should be installed regularly.	**A. 14.1 Security requirements of information systems**
Network/Communication security	**O.1**	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	**A.13 Communications Security**
Back-ups	**P.1**	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	**A.12.3 Back-Up**
Back-ups	**P.2**	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	**A.12.3 Back-Up**
Back-ups	**P.3**	Execution of backups should be monitored to ensure completeness.	**A.12.3 Back-Up**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Back-ups	**P.4**	Full backups should be carried out regularly.	**A.12.3 Back-Up**
Mobile/Portable devices	**Q.1**	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	**A. 6.2 Mobile devices and teleworking**
Mobile/Portable devices	**Q.2**	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	**A. 6.2 Mobile devices and teleworking**
Mobile/Portable devices	**Q.3**	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	**A. 6.2 Mobile devices and teleworking**
Application lifecycle security	**R.1**	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.2**	Specific security requirements should be defined during the early stages of the development lifecycle.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.3**	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.4**	Secure coding standards and practises should be followed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.5**	During the development, testing and validation against the implementation of the initial security requirements should be performed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Data deletion/disposal	**S.1**	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**
Data deletion/disposal	**S.2**	Shredding of paper and portable media used to store personal data shall be carried out.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**
Physical security	**T.1**	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	**A.11 – Physical and environmental security**

A.2 Proposed Measures for Medium Risk Level

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Security policy and procedures for the protection of personal data	**A.3**	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	**A.5 Security policy**
Security policy and procedures for the protection of personal data	**A.4**	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	**A.5 Security policy**
Security policy and procedures for the protection of personal data	**A.5**	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	**A.5 Security policy**
Roles and responsibilities	**B.3**	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.	**A.6.1.1 Information security roles and responsibilities**
Access control policy	**C.2**	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.	**A.9.1.1 Access control policy**
Access control policy	**C.3**	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.	**A.9.1.1 Access control policy**
Resource/asset management	**D.3**	Roles having access to certain resources should be defined and documented.	**A.8 Asset management**
Change management	**E.3**	A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.	**A. 12.1 Operational procedures and responsibilities**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Data processors	**F.4**	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.	**A.15 Supplier relationships**
Incidents handling / Personal data breaches	**G.3**	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.	**A.16 Information security incident management**
Business continuity	**H.2**	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.	**A. 17 Information security aspects of business continuity management**
Business continuity	**H.3**	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.	**A. 17 Information security aspects of business continuity management**
Confidentiality of personnel	**I.2**	Prior to up taking their duties employees should be asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.	**A.7 Human resource security**
Training	**J.2**	The organization should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.	**A.7.2.2 Information security awareness, education and training**
Access control and authentication	**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.	**A.9 Access control**
Access control and authentication	**K.6**	User passwords must be stored in a "hashed" form.	**A.9 Access control**
Logging and monitoring	**L.3**	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.	**A.12.4 Logging and monitoring**
Logging and monitoring	**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.	**A.12.4 Logging and monitoring**
Logging and monitoring	**L.5**	A monitoring system should process the log files and produce reports on	**A.12.4 Logging and monitoring**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
		the status of the system and notify for potential alerts.	
Server/Database security	**M.3**	Encryption solutions should be considered on specific files or records through software or hardware implementation.	**A. 12 Operations security**
Server/Database security	**M.4**	Encrypting storage drives should be considered	**A. 12 Operations security**
Server/Database security	**M.5**	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information	**A. 12 Operations security**
Workstation security	**N.6**	Anti-virus applications and detection signatures should be configured on a daily basis.	**A. 14.1 Security requirements of information systems**
Network/Communication security	**O.2**	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.	**A.13 Communications Security**
Network/Communication security	**O.3**	Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.	**A.13 Communications Security**
Network/Communication security	**O.4**	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.	**A.13 Communications Security**
Back-ups	**P.5**	Backup media should be regularly tested to ensure that they can be relied upon for emergency use.	**A.12.3 Back-Up**
Back-ups	**P.6**	Scheduled incremental backups should be carried out at least on a daily basis.	**A.12.3 Back-Up**
Back-ups	**P.7**	Copies of the backup should be securely stored in different locations.	**A.12.3 Back-Up**
Back-ups	**P.8**	In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the data controller.	**A.12.3 Back-Up**
Mobile/Portable devices	**Q.4**	Specific roles and responsibilities regarding mobile and portable device	**A. 6.2 Mobile devices and teleworking**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
		management should be clearly defined.	
Mobile/Portable devices	**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.	**A. 6.2 Mobile devices and teleworking**
Mobile/Portable devices	**Q.6**	Mobile devices should support separation of private and business use of the device through secure software containers.	**A. 6.2 Mobile devices and teleworking**
Mobile/Portable devices	**Q.7**	Mobile devices should be physically protected against theft when not in use.	**A. 6.2 Mobile devices and teleworking**
Application lifecycle security	**R.6**	Vulnerability assessment, application and infrastructure penetration testing should be performed by a trusted third party prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.7**	Periodic penetration testing should be carried out.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.8**	Information about technical vulnerabilities of information systems being used should be obtained.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Application lifecycle security	**R.9**	Software patches should be tested and evaluated before they are installed in an operational environment.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
Data deletion/disposal	**S.3**	Multiple passes of software-based overwriting should be performed on all media before being disposed.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**
Data deletion/disposal	**S.4**	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**
Physical security	**T.2**	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate.	**A.11 – Physical and environmental security**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Physical security	**T.3**	Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored	**A.11 – Physical and environmental security**
Physical security	**T.4**	Intruder detection systems should be installed in all security zones.	**A.11 – Physical and environmental security**
Physical security	**T.5**	Physical barriers should, where applicable, be built to prevent unauthorized physical access.	**A.11 – Physical and environmental security**
Physical security	**T.6**	Vacant secure areas should be physically locked and periodically reviewed	**A.11 – Physical and environmental security**
Physical security	**T.7**	An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room	**A.11 – Physical and environmental security**
Physical security	**T.8**	External party support service personnel should be granted restricted access to secure areas.	**A.11 – Physical and environmental security**

A.3 Proposed Measures for High Risk Level

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Security policy and procedures for the protection of personal data	**A.6**	The security policy should be reviewed and revised, if necessary, on a semester basis.	**A.5 Security policy**
Roles and responsibilities	**B.4**	The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.	**A.6.1.1 Information security roles and responsibilities**
Roles and responsibilities	**B.5**	Conflicting duties and areas of responsibility, for examples the roles of security officer, security auditor, and DPO, should considered to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.	**A.6.1.1 Information security roles and responsibilities**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Access control policy	**C.4**	Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.	**A.9.1.1 Access control policy**
Resource/asset management	**D.4**	IT resources should be reviewed and updated on annual basis.	**A.8 Asset management**
Data processors	**F.5**	The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.	**A.15 Supplier relationships**
Incidents handling / Personal data breaches	**G.4**	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.	**A.16 Information security incident management**
Business continuity	**H.4**	Specific personnel with the necessary responsibility, authority and competence to manage business continuity in the event of an incident/personal data breach should be nominated.	**A. 17 Information security aspects of business continuity management**
Business continuity	**H.5**	An alternative facility should be considered, depending on the organization and the acceptable downtime of the IT system.	**A. 17 Information security aspects of business continuity management**
Confidentiality of personnel	**I.3**	Employees involved in high risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).	**A.7 Human resource security**
Training	**J.3**	A training plan with defined goals and objectives should be prepared and executed on an annual basis.	**A.7.2.2 Information security awareness, education and training**
Access control and authentication	**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.	**A.9 Access control**
Access control and authentication	**K.8**	Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.	**A.9 Access control**
Server/Database security	**M.6**	Techniques supporting privacy at the database level, such as	**A. 12 Operations security**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
		authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.	
Workstation security	**N.7**	It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).	**A. 14.1 Security requirements of information systems**
Workstation security	**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.	**A. 14.1 Security requirements of information systems**
Workstation security	**N.9**	Full disk encryption should be enabled on the workstation operating system drives	**A. 14.1 Security requirements of information systems**
Network/Communication security	**O.5**	Connection to the internet should not be allowed to servers and workstations used for the processing of personal data.	**A.13 Communications Security**
Network/Communication security	**O.6**	The network of the information system should be segregated from the other networks of the data controller.	**A.13 Communications Security**
Network/Communication security	**O.7**	Access to the IT system should be performed only by pre-authorized devices and terminal using techniques such as MAC filtering or Network Access Control (NAC)	**A.13 Communications Security**
Back-ups	**P.9**	Copies of backups should be encrypted and securely stored offline as well.	**A.12.3 Back-Up**
Mobile/Portable devices	**Q.8**	Two factor authentication should be considered for accessing mobile devices	**A. 6.2 Mobile devices and teleworking**
Mobile/Portable devices	**Q.9**	Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.	**A. 6.2 Mobile devices and teleworking**
Data deletion/disposal	**S.5**	Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**

MEASURE CATEGORY	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Data deletion/disposal	**S.6**	If a third party, therefor data processor, is being used for destruction of media or paper based files, it should be considered that the process takes place at the premises of the data controller (and avoid off-site transfer of personal data.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or re-use of equipment**

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

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

TP-02-18-047-EN-N

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

ISBN: 978-92-9204-251-6
DOI: 10.2824/569768