EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ONLINE PLATFORM FOR SECURITY OF PERSONAL DATA PROCESSING

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

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

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

CONTRIBUTORS

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

EDITORS

Prokopios Drogkaris (ENISA) and Athena Bourka (ENISA)

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-327-8, DOI 10.2824/3000

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As security of personal data processing is a key obligation for data controllers and processors under the General Data Protection Regulation [1] Article 32, ENISA has proposed in 2018 a risk-based approach for the adoption of security measures for the protection of personal data. Following this, a number of use cases has also been provided to demonstrate the use of the risk-based approach in practice, together with an analysis of the different security measures (and possible implementation options). In order to support the practical implementation of the aforementioned ENISA's guidance, an online platform was developed, which consolidates and simplifies the risk-based adoption of security measures for all interested parties.

This report presents the focus and main functionalities of the ENISA's online platform for the security of personal data processing. This platform is only one tool, which cannot replace the need of a greater compliance and accountability framework for personal data protection on the data controllers or data processors side. Moreover, the use of the ENISA approach can be beneficial for organisations only if the special characteristics of personal data security are adequately embraced and integrated with security risk management methodologies.

In order to do so, it is essential to continue working on use cases and best practice examples of personal data security risk assessments in practice. It is also important to explore the convergence of relevant frameworks with regard to standardisation and certification frameworks in the field.

Taking the above considerations into account, ENISA has drawn the following conclusions and recommendations for relevant stakeholders:

- Data controllers (e.g. SMEs), associations and competent EU bodies should work towards common use cases and examples for personal data security, while supporting broader security risk assessment frameworks that embed data protection requirements.
- Competent EU bodies and Data Protection Authorities should develop practical guidance documents that will be able to support and assist different types of data controllers on the selection of appropriate and adequate security measures.
- The research community and standardization bodies should continue working on giving technical solutions to ever increasing security threats in different areas of security measures and privacy enhancing technologies, with the support of competent EU bodies and the European Commission, in terms of policy guidance and funding.
- The European Commission, Data Protection Authorities and Competent EU bodies should explore the possible synergies between different certification frameworks as regards the security of personal data processing.

1. INTRODUCTION

1.1 BACKGROUND

Information security risk management is the process of identifying, quantifying, and managing the IT security risks that an organisation faces. Security risk assessment is at the heart of this process, followed by risk treatment, acceptance and communication. An information security risk is the combination of the likelihood that a threat materialises and the impact that such a threat would have for the organisation. Well-known standards, such as ISO/IEC 27005:2018 [2] and NIST 800-39 [3], have contributed towards relevant methods, tools and practical implementation.

Based on GDPR Art.32 provisions, personal data security is strongly risk-based but a personal data security risk management system needs to adapt to the specificities of personal data [4]. Evidently, as a first point, in the context of the risk assessment, the impact needs to be considered towards the individuals (and their rights and freedoms), hence taking a different angle from the classic security risk assessment. The scale is not necessarily relevant towards this end, e.g. the impact may be high even if the number of affected persons is low. In addition, possible secondary effects may also need to be considered (e.g. when assessing possible impacts of a personal data breach). Moreover, after the evaluation of risks, the risk management process varies from typical security risk management. For example, risk acceptance would not be possible in cases where risks to individuals are concerned. In addition, risk treatment would need to integrate privacy enhancing technologies, e.g. technologies reducing the identifiability of data subjects (and not necessarily qualifying under the “classic” Confidentiality, Integrity, Availability (CIA) triad - protection technologies) [5].

Security of personal data processing is a key obligation for data controllers and processors under the General Data Protection Regulation (GDPR) [1]. In particular, data controllers and processors are required to implement technical and organisational measures that are appropriate to the risk presented to the rights and freedoms of individuals (article 32 GDPR).

In an effort to support organisations and especially Small and Medium Enterprises (SMEs) in the EU in complying with the GDPR obligations, ENISA has proposed a risk-based approach for the adoption of security measures for the protection of personal data [4]. A number of use cases has also been provided to demonstrate the use of the risk-based approach in practice, together with an analysis of the different security measures (and possible implementation options) [6] & [7]. The proposed security measures are based on the ISO 27000 standards family, incorporating also additional controls that are specific to the processing of personal data.

In order to support the practical implementation of the aforementioned ENISA guidance, ENISA decided under its 2019 work programme to provide an online platform, which would consolidate and simplify the risk-based adoption of security measures for all interested parties. This report presents the focus and main functionalities of the ENISA’s online platform for the security of personal data processing.

1.2 SCOPE

The scope of the ENISA’s online platform for the security of personal data processing (hereinafter “online platform”) is to provide a practical tool for security risk assessment and subsequent adoption of security measures for the protection of personal data, based on the relevant ENISA methodology [4]. The on line platform is available under https://www.enisa.europa.eu/risk-level-tool/.

In practice, the online platform incorporates the different steps for a risk-based approach proposed by ENISA and guides any interested organisation (e.g. a data controller or processor) through an assessment of the level of security risk, leading to a list of proposed security measures appropriate to the risk presented. In addition, the platform provides the possibility of a security self-assessment, i.e. assessing the measures that have been adopted by an organisation vis-à-vis the perceived/identified level of risk.

The target audience of ENISA's online platform is any organisation acting as a controller or processor that is interested in assessing the security risks and adopt security measures for the protection of personal data. The platform may also be of interest to Data Protection Authorities, as a tool that can support security of personal data processing.

It should be noted that ENISA's online platform is explicitly focused on the security of personal data processing and does not constitute a Data Protection Impact Assessment (DPIA) tool, which is of broader nature[1]. However, ENISA's platform could be utilised in the context of a DPIA tool, as far as security of personal data processing is concerned.

For further information regarding the underlying methodology upon which the ENISA's online platform is based, the relevant ENISA's guidelines should be consulted [4].

1.3 STRUCTURE OF THE DOCUMENT

This report provides supporting information with regard to ENISA's online platform for the security of personal data processing. The structure of the remainder of the report is as follows:

- Section 2 provides a summary of ENISA's guidelines on security of personal data processing (which forms the basis of the platform's functionality).
- Section 3 presents the main functionality of the platform, including relevant screenshots and explanatory information.
- Section 4 draws some conclusions and recommendations with regard to further steps in the field.

The online platform for the security of personal data processing is part of the work of ENISA in the area of privacy and data protection[2], which focuses on analysing technical solutions for the implementation of GDPR, privacy by design and security of personal data processing.

[1] See for example, the DPIA tool provided by the French Data Protection Authority (CNIL), https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carry-out-data-protection-impact
[2] https://www.enisa.europa.eu/topics/data-protection

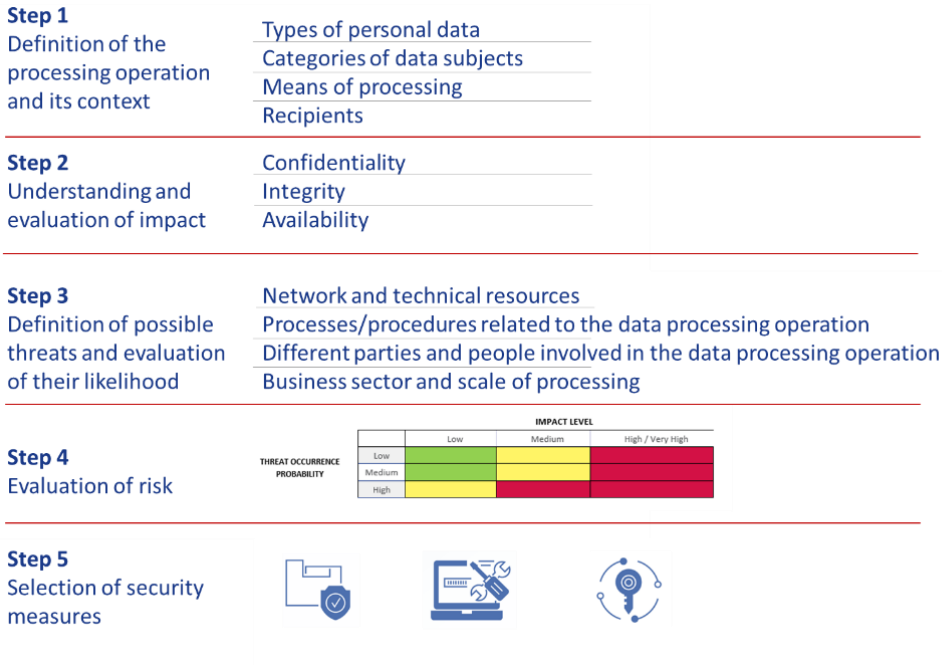
2. GUIDELINES ON THE SECURITY OF PERSONAL DATA PROCESSING

2.1 INTRODUCTION

This Chapter provides an overview of ENISA's guidelines on security of personal data processing, which mainly includes a risk-based approach towards adopting security measures [4].

In particular, ENISA has presented a simplified approach in order to guide organisations (in their role as controllers or processors) through their specific data processing operations and assist them in understanding and evaluating the relevant security risks. The proposed approach is based on four main steps, as depicted in Figure 1 (steps 1 to 4).

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



After the evaluation of the risk, an additional step (step 5 in Figure 1) is the selection of security measures (that are appropriate to the risk presented).

In the next sections, the different steps of ENISA's proposed methodology are explained in more detail. The terms organisation and controller/processor are used interchangeably to describe the entity that conducts the risk assessment for the security of personal data.

2.2 STEP 1: DEFINITION OF THE PROCESSING OPERATION AND ITS CONTEXT

This step is the starting point of the risk assessment and is fundamental for the data controller/processor in order to define the boundaries of the data processing system (under

assessment) and its relevant context. In doing so, the organisation needs to consider the different phases of data processing (collection, storage, use, transfer, disposal, etc.) along with relevant aspects such as data recipients, means used for processing, etc.

The following questions (Table 1) need, as a minimum, to be asked and clearly understood by the data controller/processor. Relevant examples and practical guidance, through use cases, can be sourced in [6].

Table 1: Minimum set of questions for defining the processing operation and its context

	Question	Purpose
1.	What is the personal data processing operation?	To realise if different risk assessment processes should run for different data processing operations.
2.	What are the types of personal data processed?	To understand the types of operations based on the data types; to get an indication of potential risk levels (as regards the types of data).
3.	What is the purpose of the processing?	To understand the limits of the data processing operation (as regards the purpose).
4.	What are the means used for the processing of personal data?	To define the means used for the data processing operations and their different types (in house resources, outsourced tools, etc.).
5.	Where does the processing of personal data take place?	To determine the location of the personal data processing.
6.	Which are the categories of data subjects?	To define the types of data subjects (clients, customers, etc.) involved in the data processing operation.
7.	Which are the recipients of the data?	To define the recipients of the data for capturing the authorized transfers of these data and the conditions of these transfers.

The result of this step is a more thorough understanding of the data processing operation (for the controller/processor), which forms the basis of the analysis in the following steps of the assessment.

2.3 STEP 2: UNDERSTANDING AND EVALUATING THE IMPACT

Once the processing operation and its context are well defined, the data controller/processor is guided to evaluate the potential impact to the rights and freedoms of individuals that a security incident (related to the data processing system) might bring. The security incident may be associated with any type of breach of confidentiality, integrity or availability of personal data.

Due to the ad-hoc nature and diversity of personal data processing operations, only a *qualitative approach* can be used, based on the overall understanding (by the organisation) of its specific data processing operation. To this end, the evaluation of the impact is based on a number of parameters, such as the type and volume of personal data, the criticality of the processing operation, special characteristics of the data controller/processor, special characteristics of the data subjects, as well as the level of identifiability of data subjects.

Following this assessment, the controller/processor is finally asked to assess the impact, based on four predefined levels, i.e. low, medium, high and very high, as shown in Table 2 below.

Table 2: Levels of impact

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

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

2.4 STEP 3: DEFINITION OF POSSIBLE THREATS AND EVALUATION OF THEIR LIKELIHOOD

A threat is any circumstance or event, which has the potential to adversely affect the security of personal data. At this step, the goal for the data controller/processor is to understand the threats related to the overall environment of the personal data processing (external or internal) and assess their likelihood (threat occurrence probability). Varying levels and types of threats to the confidentiality, integrity and availability of personal data could be considered in this respect.

Similar to the case of the evaluation of impact, the assessment of threat occurrence probability can only be qualitative, as it is very much related to the specific personal data processing environment. In the context of ENISA's approach, three levels of threat occurrence probability are defined, namely:

- Low: the threat is unlikely to materialise.
- Medium: it is possible that the threat materialises.
- High: the threat is likely to materialise.

To simplify the process for SMEs, the ENISA's approach defines four areas of assessment for threat occurrence probability, 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.

For each of these areas of assessment, a number of guiding questions is also provided, as presented in Table 3 below.

Table 3: Guiding questions for assessing threat occurrence probability

A. Network and technical resources (hardware and software)	
1.	Is any part of the processing of personal data performed through the internet?
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)?
3.	Is the personal data processing system interconnected to another external or internal (to your organisation) IT system or service?
4.	Can unauthorized individuals easily access the data processing environment?
5.	Is the personal data processing system designed, implemented or maintained without following relevant best practices?
B. Processes/procedures related to the data processing operation	
6.	Are the roles and responsibilities with regard to personal data processing vague or not clearly defined?
7.	Is the acceptable use of the network, system and physical resources within the organisation ambiguous or not clearly defined?
8.	Are the employees allowed to bring and use their own devices to connect to the personal data processing system?
9.	Are employees allowed to transfer, store or otherwise process personal data outside the premises of the organisation?
10.	Can personal data processing activities be carried out without log files being created?
C. Different parties and people involved in the processing operation	
11.	Is the processing of personal data performed by a non-defined number of employees?
12.	Is any part of the data processing operation performed by a contractor/third party (data processor)?
13.	Are the obligations of the parties/persons involved in personal data processing ambiguous or not clearly stated?
14.	Is personnel involved in the processing of personal data unfamiliar with information security matters?
15.	Do persons/parties involved in the data processing operation neglect to securely store and/or destroy personal data?
D. Business sector and scale of the processing	
16.	Do you consider your business sector as being prone to cyberattacks?
17.	Has your organisation suffered any cyberattack or other type of security breach over the last two years?
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?
19.	Does a processing operation concern a large volume of individuals and/or personal data?
20.	Are there any security best practices specific to your business sector that have not been adequately followed?

Using the answers to the aforementioned questions as drivers/indicators, the controller/processor assesses the threat occurrence probability for each of the four areas mentioned above. At the end, the threat occurrence probability is obtained as the highest of the scores obtained per area.

2.5 EVALUATION OF RISK

After evaluating the impact of the personal data processing operation and the relevant threat occurrence probability, the final evaluation of risk is possible, as shown in Figure 3 and Table 4 below.

Figure 3: Evaluating risk

Table 4: Levels of risk

		Impact Level		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low			
	Medium			
	High			

Legend

Low Risk | Medium Risk | High Risk

The controller/processor can always modify the level of risk based on its particular circumstances and providing relevant justification for this modification.

2.6 STEP 5: SELECTION OF APPROPRIATE SECURITY MEASURES

Following the evaluation of the risk level, the data controller/processor can proceed with the selection of appropriate security measures for the protection of personal data. Two broad categories of measures, organisational and technical ones, which are further divided in specific categories, are considered (Table 5). In principle, they follow the categorization given in ISO/IEC 27001:2013 Annex A and ISO/IEC 27002:2013.

Table 5: Categories of security measures

Organisational Security Measures Categories	Technical Security Measures Categories
Security management	**Access control and authentication**
● Security policy and procedures for the protection of personal data	**Logging and monitoring**
● Roles and responsibilities	**Security of data at rest**
● Access control policy	● Server/Database security
● Resource/asset management	● Workstation security
● Change management	**Network/Communication security**
● Data processors	**Back-ups**
Incident response and business continuity	**Mobile/Portable devices**
● Incidents handling / Personal data breaches	**Application lifecycle security**
● Business continuity	**Data deletion/disposal**
Human Resources	**Physical security**
● Confidentiality of personnel	
● Training	

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 organisation 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[3] or the NIS Directive[4].

[3] Directive 2002/58/EC on privacy and electronic communications: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002L0058
[4] 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

3. ONLINE PLATFORM

3.1 INTRODUCTION

ENISA's online platform for the security of personal data processing is based on the ENISA guidelines presented in Chapter 2 and aims to provide a simple tool supporting personal data security.

The on line platform is available under https://www.enisa.europa.eu/risk-level-tool/.

This Section presents the main functionality of the online platform, which consists mainly of two parts:

- A security risk-assessment approach for personal data processing.
- A security self-assessment tool for data controllers/processors.

While the security risk assessment approach practically implements the relevant ENISA's guidelines (see in Chapter 2), the self-assessment tool aims to provide an additional control mechanism for data controllers/processor for assessing the adopted security measures (see also relevant finding under ENISA's 2019 report [7]).

Additional material and links to ENISA's relevant work is also available through the platform.

It should be noted that none of the data/information entered in the platform is saved by/at the platform; therefore all entered data/information become unavailable once the browser is closed (the users of the platform are, thus, advised to run this exercise all iat once). Still, in order to support data controllers/processors, the platform offers the possibility to export the results of both parts (security risk assessment and self-assessment tool) in PDF format.

The next sections present in more detail the different functions of the online platform.

3.2 HOMEPAGE

The homepage of the tool displays the four different options that are available to the user:

- Evaluating the level of risk for a personal data processing operation.
- (Self)-assessing implemented security measures.
- Overview of the ENISA's guidelines upon which the risk assessment methodology is based.
- Relevant ENISA studies in the field.

Figure 2: Home Page Overview

The next Sections describe each of these options in more detail.

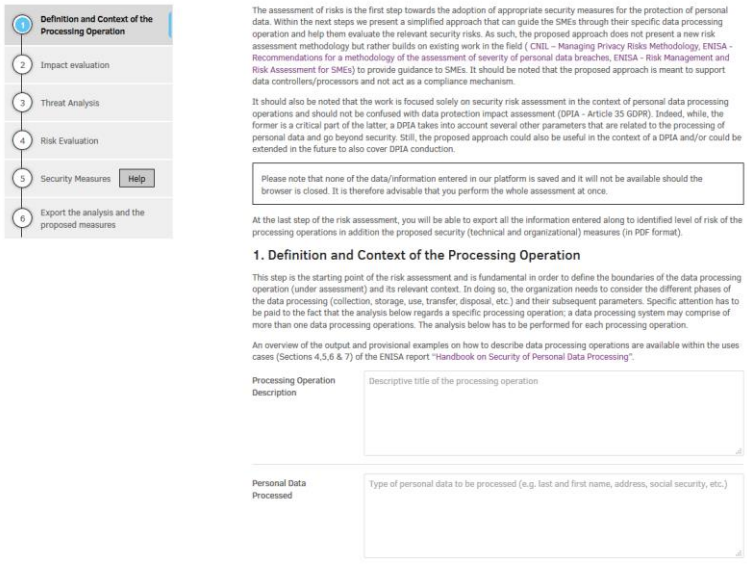
3.3 EVALUATING THE LEVEL OF RISK FOR A PERSONAL DATA PROCESSING OPERATION

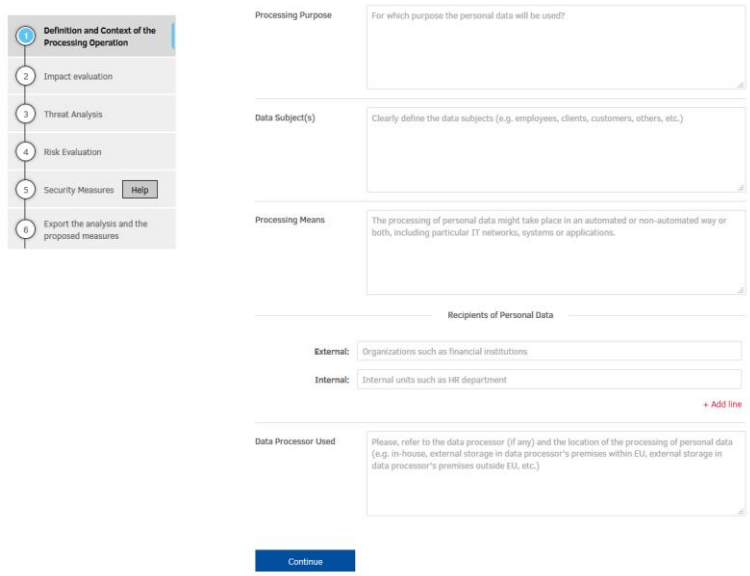
As already mentioned, the risk assessment option implements ENISA's guidelines for security risk assessment of personal data processing [3]. All different steps of these guidelines are subsequently embedded in the online platform.

3.3.1 Definition and Context of the processing operation

This step is linked to Step 1 of ENISA's guidelines, as discussed in Section 2.2 of this document. Through relevant input text boxes, the user (i.e. from an organisation acting as controller or processor) is asked to define the boundaries of the data processing operation under assessment.

Figure 3: Definition and Context of the processing operation



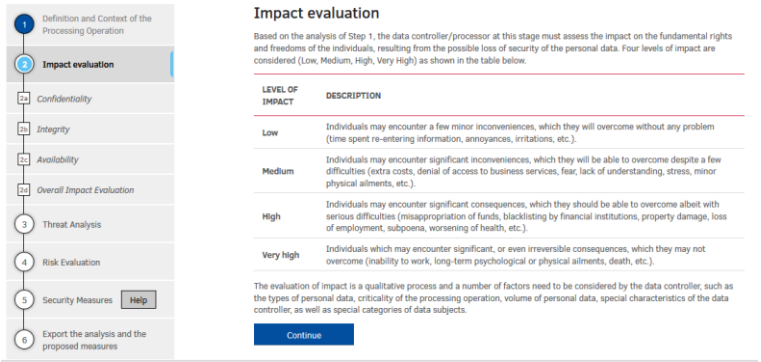


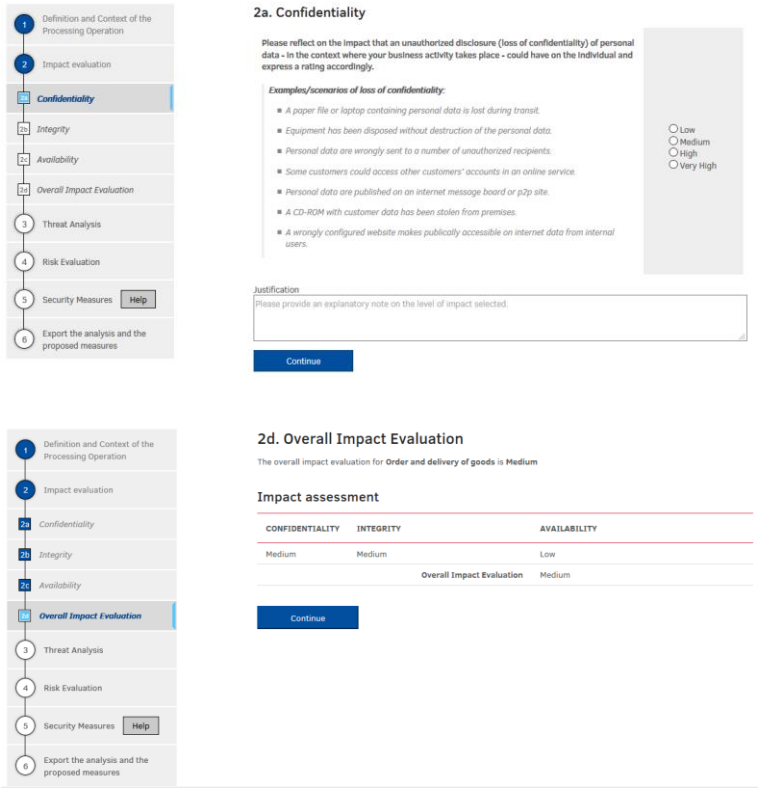
This step supports the user to understand better the data processing operation under assessment.

3.3.2 Impact evaluation

The next step is linked to Step 2 of ENISA's guidelines, as discussed in Section 2.3 of this document. Firstly, user is presented with information on the four levels of impact that are available. Next, he or she is asked to assess the impact for data confidentiality, then integrity and then availability. Apart from selecting the level of impact for each assessment, the user is also able to optionally provide justification on the level of impact selected. Lastly, the user is presented with the overall impact evaluation of the processing operation, based on the selections he or she made in the previous sub-steps.

Figure 4: Impact Evaluation Overview



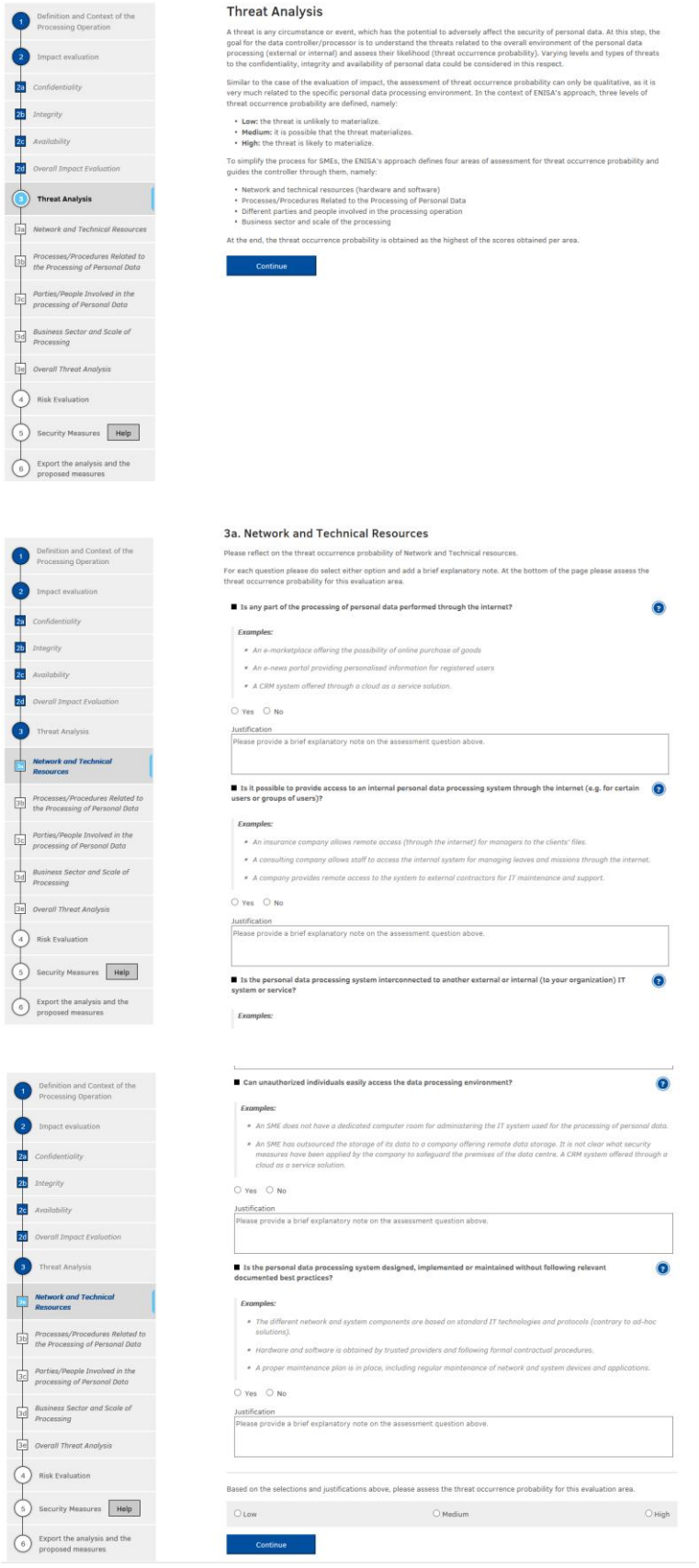


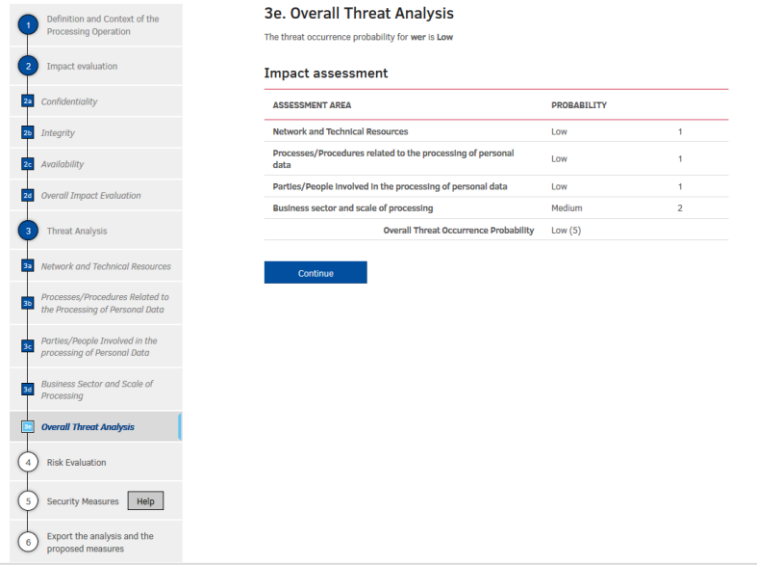
In all phases of this step, the user is supported by relevant examples.

3.3.3 Threat Analysis

The next step is linked to Step 3 of ENISA's guidelines, as discussed in Section 2.4 of this document. Firstly, the user is presented with information on the three levels of threat occurrence probability and the four areas of assessment. Next, for each area he or she is presented with guiding questions and at the end he or she is asked to assess the threat occurrence probability for the specific evaluation area. Under each guiding question, further to the examples provided, the user is also able to optionally select "yes" or "no" and provide a short justification. Similarly to the impact evaluation in Section 3.3.2, this input, even if it is not part of the methodological steps described in Chapter 2, is meant to support the data controller/processor when reviewing the outcome of the evaluation. Following the completion of all four assessment areas, the user is presented with the overall threat occurrence probability of the processing operation, based on the selections he or she made in the previous sub-steps.

Figure 5: Threat Analysis Overview



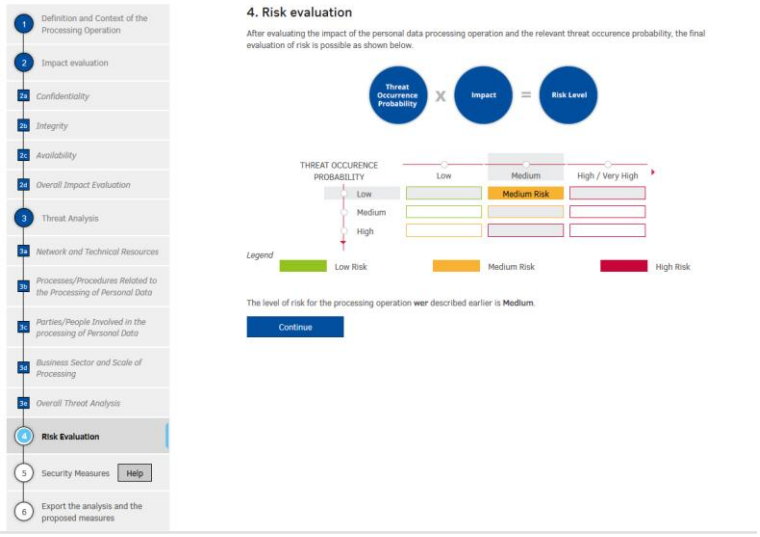


At the end of this step, the main part of the risk assessment is concluded.

3.3.4 Risk Evaluation

The next step is linked to Step 4 of ENISA's guidelines, as discussed in Section 2.5 of this document. Based on the impact level identified in Step 2 and the threat occurrence probability identified in Step 3, the user is presented with the overall risk level of the specific processing operation.

Figure 6: Risk Evaluation

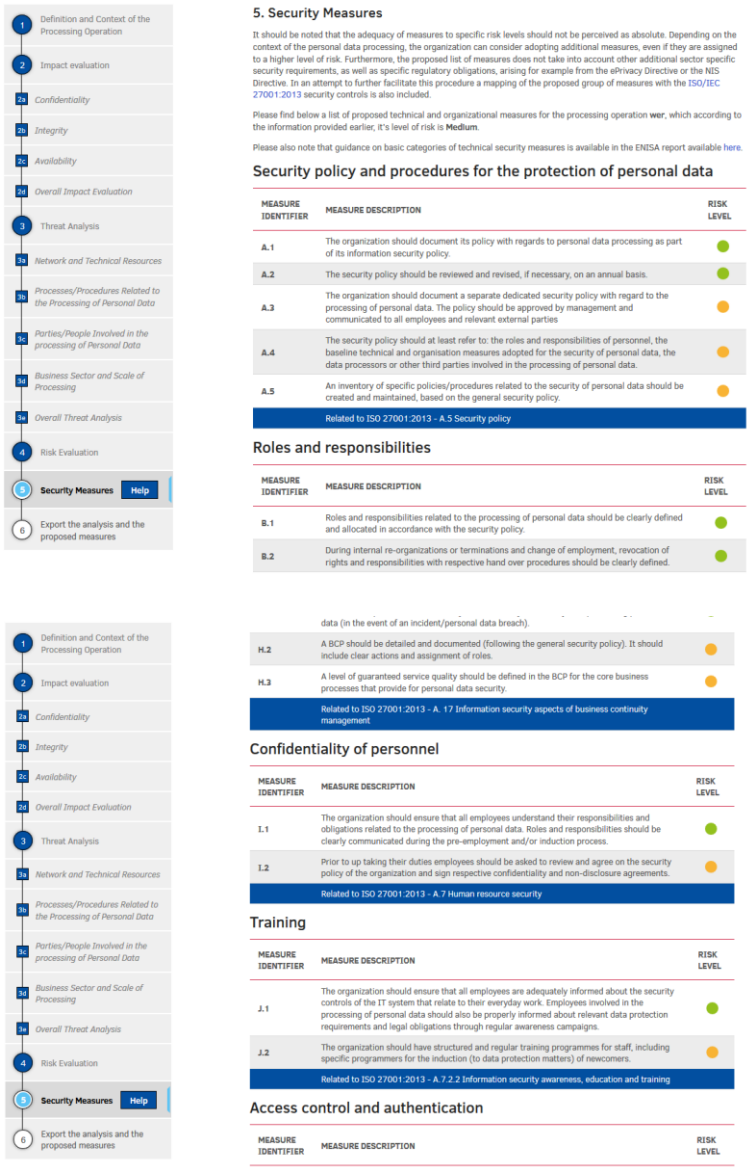


Following an obtained level of risk, the controller/processor may modify this risk level, depending on the specific processing context and provided that relevant justification is available.,

3.3.5 Security Measures

The next step is linked to Step 5 of ENISA's guidelines, as discussed in Section 2.6 of this document. Based on the identified level of risk, a list of appropriate technical and organisational security measures is presented to the user.

Figure 7: Security Measures

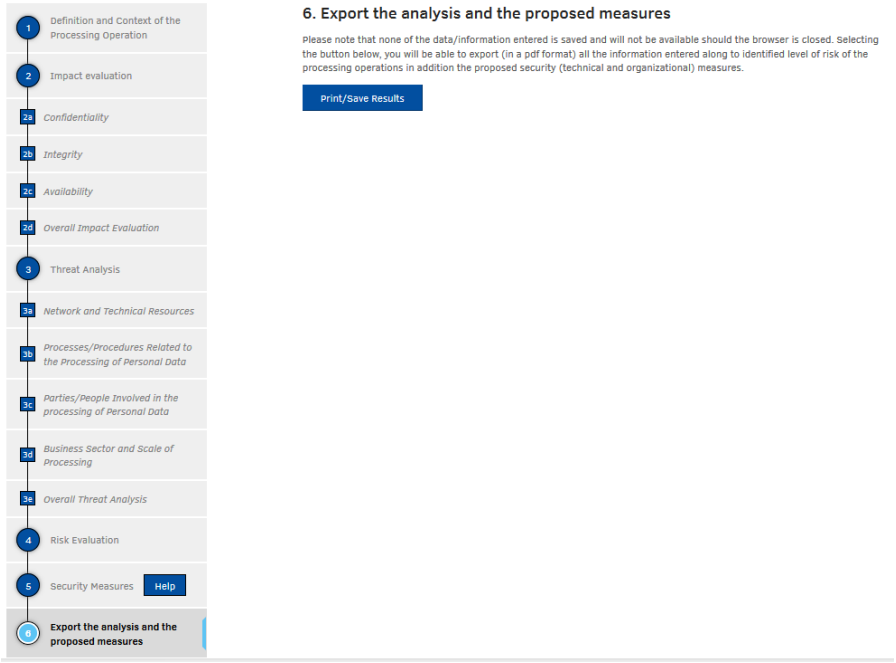


The proposed security measures span across different categories and levels of detail, as explained in Section 2.6 of this document.

3.3.6 Export of the analysis

The last step of the security risk assessment in the online platform is the export in PDF format of all the input that the user provided for the specific processing operation, in addition to the identified level of impact, the threat occurrence probability, the level of risk and the proposed technical and organisational security measures.

Figure 8: Export of the analysis



This export providers to the user (organisation acting as data controller/processor) with the detailed analysis of the performed risk-assessment on the basis of ENISA's guidelines [3].

The data/information provided by the user and the results of the analysis are not stored in the online platform (and, therefore, are not anymore available to the user after the browser is closed).

3.4 SELF-ASSESSMENT

The self-assessment option of the online platform is complimentary to the security risk assessment function described in 3.3. It was developed in an attempt to continue supporting the data controllers/processor after the initial risk assessment (see also findings under [7] for putting forward practical self-evaluation tools for controllers/processors).

In this case, the user is asked to select the identified level of risk (obtained through a prior security risk assessment) and provide a short description of the processing operation. Following this input, the user is then presented with all applicable (to the level of risk) technical and organisational measures and is able to select the ones already implemented. The final step of this exercise is a PDF document, which lists the implemented measures and the ones pending implementation. This output can either serve as a self-assessment of the measures to be implemented or as a continuous progress monitoring of the steps taken by the data controller/processor towards deployment of the all proposed measures.

Figure 9: Self-Assessment Overview

Following the assessment of the level of risk for a given processing operation and the proposal for appropriate security measures (both technical and organizational), the data controller/processor might need to (re)check the status of adoption/implementation of the proposed measures.

Through this self-assessment mechanism, the data controller/processor is able to introduce the level of risk for a personal data processing operation and provide a short description of it. Then, by selecting the button below, she/he is then able to select which of the proposed measures are already implemented and then be left with a list of those, which are still to be deployed. Once more, this list should not be perceived as absolute but as guidance based on the methodological steps proposed by ENISA. Similar methodologies on the evaluation of risk have also been published by CNIL, ICO etc.

Level of risk

Please select the level of risk

Processing operation

Please input the processing operation

Display proposed security measures

Please click the checkbox for each of the security measures that you are already implementing.

Security policy and procedures for the protection of personal data

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

Roles and responsibilities

IMPLEMENTED?	MEASURE IDENTIFIER	MEASURE DESCRIPTION	RISK LEVEL
☐	B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	
☐	B.2	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	
☐	B.3	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.	
		Related to ISO 27001:2013 - A.6.1.1 Information security roles and responsibilities	

Implemented

Security policy and procedures for the protection of personal data

Measure Identifier	Measure Description	Risk level
A.1	The organization should document its policy with regards to personal data processing as part of its information security policy.	
A.2	The security policy should be reviewed and revised, if necessary, on an annual basis.	
A.3	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	
	Related to ISO 27001:2013 - A.5 Security policy	

Resource/asset management

Measure Identifier	Measure Description	Risk level
D.2	IT resources should be reviewed and updated on regular basis.	
	Related to ISO 27001:2013 - A.8 Asset management	

Change management

Measure Identifier	Measure Description	Risk level
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.	
	Related to ISO 27001:2013 - A. 12.1 Operational procedures and responsibilities	

Pending implementation and deployment

Measure Identifier	Measure Description	Risk level
A.4	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	
A.5	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	
	Related to ISO 27001:2013 - A.5 Security policy	

Roles and responsibilities

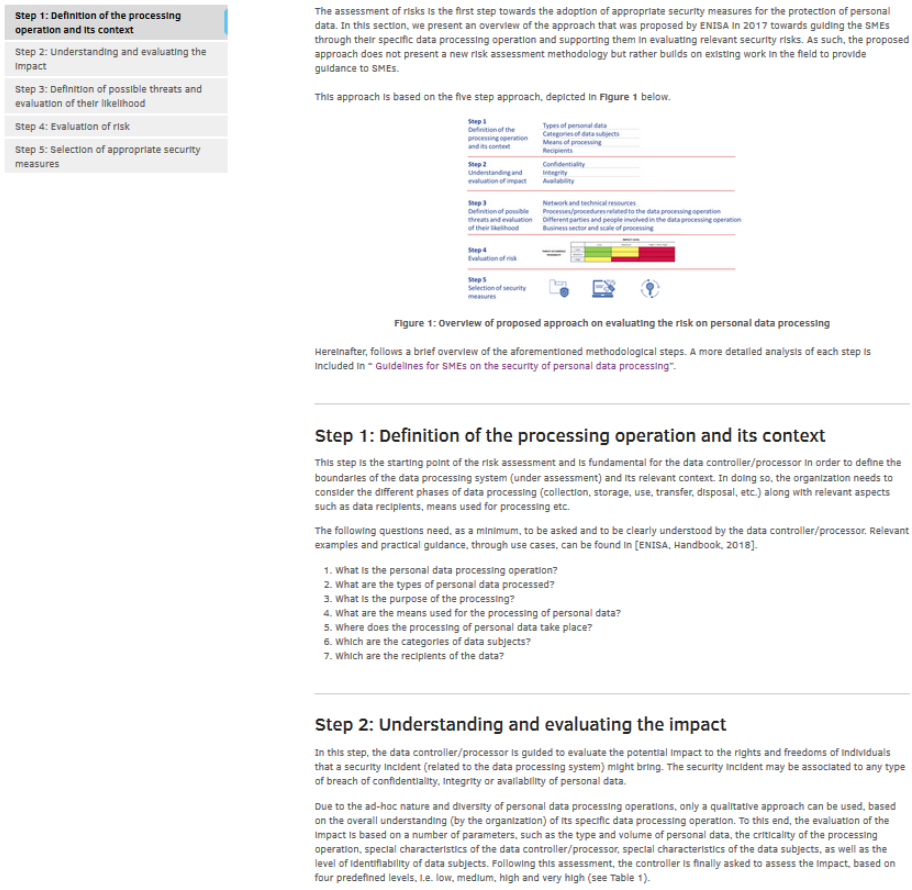
Measure Identifier	Measure Description	Risk level
B.1	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	

Depending on the specific context of the data processing operation, the controller/processor may choose to implement further measures (e.g. corresponding to higher levels of risk).

3.5 OVERVIEW OF METHODOLOGY

This part of the online platform provides a concise overview of the ENISA's guidelines, as presented in Section 2 of this document. It is meant to familiarise users with the different methodological steps and serve as a quick reference point.

Figure 10: Overview of methodology

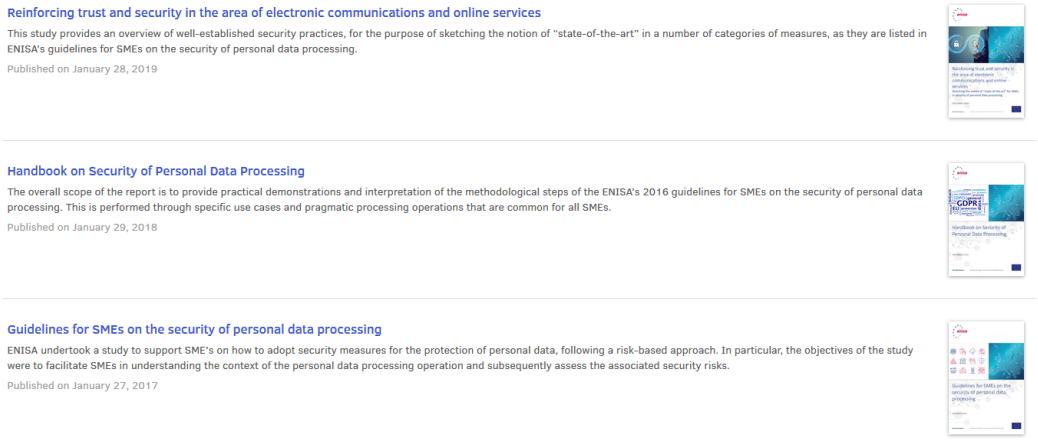


The presentation follows strictly ENISA's guidelines in this field [3].

3.6 RELEVANT ENISA STUDIES

This part of the online platform provides an overview of relevant ENISA publications in the area of security of personal data processing. In particular the following publications are listed:

Figure 10: Relevant ENISA studies



This part will be updated to reflect further ENISA's work in the field.

4. CONCLUSIONS AND RECOMMENDATIONS

With the development of an online platform for the security of personal data processing, ENISA concludes a 4-year work thread in the area of security of personal data processing. Starting from the development of a risk assessment approach, extending to the presentation of specific use case examples and the definition of available security measures, the platform depicts ENISA's proposal towards considering security requirements for data protection in a simple and practical way.

This being said, the proposed platform is only one tool, which cannot replace the need of a greater compliance and accountability framework for personal data protection. Moreover, the exploitation of the ENISA's approach can be beneficial for organisations only if the special characteristics of personal data security are adequately embraced and integrated with security risk management methodologies that these organisations follow. In order to do so, it is essential to continue working on use cases and best practice examples of personal data security risk assessments. Lastly, it is also important to explore the convergence of relevant frameworks with regard to standardisation and certification frameworks in the field.

Taking the above considerations into account, ENISA draws in the following some subsections conclusions and recommendations for all relevant stakeholders.

4.1 RISK ASSESSMENT FRAMEWORKS AND IMPLEMENTATION

Despite its specificities, security of personal data processing cannot (and should not) be considered within an organisation as an isolated issue. However, it is not always trivial to adequately combine and embed data protection requirements within "traditional" security risk assessment methodologies. How can a tool such as ENISA's online platform for personal data processing (or other similar tools) support organisations, especially SMEs, to this end? While specific use cases can help, a broader perspective towards security and data protection risk management frameworks for SMEs could be of great value.

Data controllers (e.g. SMEs) associations and competent EU bodies should work towards common use cases and examples for personal data security, while supporting broader security risk assessment frameworks that embed data protection requirements.

Competent EU bodies and Data Protection Authorities should develop practical guidance documents that will be able to support and assist different types of data controllers on the selection of appropriate and adequate security measures.

4.2 SECURITY AND PRIVACY STANDARDS

Security and data protection risk assessment frameworks can greatly be supported by standardisation activities. While security standards in the field (such as the ISO2700 family) are well established, privacy standards do not have the same level of adoption. Towards this direction, the newly published ISO/IEC 27701:2019 [8] is a promising step, however, as also acknowledged by a relevant ENISA study on privacy standards for information security [9], a structured approach on definition, endorsement or affirmation of potential standardisation goals is still needed.

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

4.3 JOINT EFFORTS ON FUTURE CERTIFICATION SCHEMES

With the Regulation (EU) 2019/881 (Cybersecurity Act), a European framework on cybersecurity certification is established. At the same time, GDPR (in its article 42) provides specific provisions for the certification of data processing operations. While the two frameworks differ in nature and in scope, it is apparent that they could mutually benefit from a joint approach in the area of security of personal data processing. Relevant risk assessment methodologies and tools can greatly contribute towards the definition of relevant synergies in the field.

The European Commission, Data Protection Authorities and Competent EU bodies should explore the possible synergies between different certification frameworks as regards the security of personal data processing.

5. REFERENCES

[1] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," 2016.

[2] ISO/IEC, "ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management," 2018.

[3] NIST, "NIST Special Publication 800-39 - Managing Information Security Risk," 2011.

[4] ENISA, "Guidelines for SMEs on the security of personal data processing," 2017.

[5] A. Bourka and P. Drogkaris, "Security meets data protection: from risk management to systems engineering," in *15 years of ENISA: A Success story*, Publications Office of the European Union, 2019, pp. 125-135.

[6] ENISA, "Handbook on Security of Personal Data Processing," 2018.

[7] ENISA, "Reinforcing trust and security in the area of electronic communications and online services," 2019.

[8] ISO/IEC, "ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines," 2019.

[9] ENISA, "Privacy standards for information security," 2019.

TP-01-20-039-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

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

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

enisa.europa.eu

ISBN 978-92-9204-327-8
doi: 10.2824/3000