Cyber Security for Europe

D3.6

Guidelines for GDPR Compliant User Experience

Document Identification	
Due date	2020-01-31
Submission date	2020-01-30
Revision	1.0

Related WP	WP3	Dissemination Level	CO
Lead Participant	UM	Lead Author	Boštjan Kežmah (UM)
Contributing Beneficiaries	AIT, ARCH, ATOS, CNR, GUF, UM, UMU	Related Deliverables	

Abstract: These guidelines were designed as the result of the main findings of Task 3.7, part of the CyberSec4Europe project. They present a combined requirements synthesis from the GDPR, European Data Protection Board Guidelines, frameworks and up-to-date standards related to data privacy protection in the EU. The combined guidelines follow the latest standards, methods and frameworks for risk analysis. By following these guidelines, data controllers and processors can either execute data protection impact assessment or get combined guidelines for GDPR compliance. Specific requirements for Member States were addressed but not covered.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This document is the result of research and development activities in task 3.7 of the CyberSec4Europe project. Activities and results of this task were envisioned and planned for the Work Package 3 of the project between the 1st and 12th month of the project. Due to the nature of the task, the UM took the lead on this deliverable, while other partners will contribute in future work.

The guidelines were synthesized from the Asia-Pacific Economic Cooperation Privacy Guidelines [1], Generally Accepted Privacy Principles from Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) [2], ISACA Privacy Principles [3] and ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework [4] with intent to develop open, technology-neutral guidelines with the potential for compliance with existing standards and privacy frameworks other than the GDPR alone.

By following these guidelines, data controllers and processors can either execute data protection impact assessment and/or get combined guidelines for GDPR compliance. Specific requirements for the Member States were addressed but not covered.

The combined guidelines follow the latest standards, methods and frameworks for risk analysis and include a simple to follow methodology that was objectified to the largest possible extent. Partially this also includes the WP29 Guidelines [5] that were endorsed by the European Data Protection Board (EDPB).

The guidelines include a baseline of identified risk to conduct threat analysis during Data Protection Impact Assessment exercise and easy to follow instructions where additional information is needed to explain decisions taken and document analysis process. The guidelines end with required Data Protection Officer consultation template and self-assessment.

During the research, we have identified many issues with regulatory harmonization in the field of privacy in the European Union. Foreseeing further research efforts needed to fully understand the consequences of regulatory differences between the Member States lead us to design a questionnaire to gather information about additional privacy requirements in the Member States.

Preliminary results show that currently service providers and producers cannot avoid market segmentation due to differences in regulatory requirements. An example of this is the different minimum age required for consent. Businesses will need to understand the local requirements of every Member State to be able to adapt to local requirements. This leads to a lot of effort and lowers the competitiveness of the Single European Market. Even though some requirements could be collected in a single, machine-readable source, currently there is no mechanism in the project network or in the EU that would have the capabilities to ensure correct information is timely published in that central source.

Differences in the Member States regulation will also inevitably lead to difficulties in eIDAS implementations and business competitiveness between the Member States. Future research and development of Task 3.7 will focus on eIDAS privacy, security and operability and we envision to use the

whole synergic power of the project network to achieve research and development goals and support demo projects at the same time.

Document information

Contributors

Name	Partner
Boštjan Kežmah	UM
Tamara Bubnjar	UM
Marko Hölbl	UM
Marko Kompara	UM
Pasquale Annicchino	ARCH

Reviewers

Name	Partner
Elias Athanasopoulos	UCY
Alberto Lluch Lafuente	DTU
Ahad Niknia	GUF (High-level review)

History

0.01	2019-07-02	Boštjan Kežmah	1st Draft
0.02	2019-08-31	Boštjan Kežmah	Identified privacy risks baseline
0.03	2019-08-31	Boštjan Kežmah	DPIA self-assessment
0.04	2019-11-06	Tamara Bubnjar	Privacy frameworks selection and assessment
0.05	2019-11-13	Tamara Bubnjar	Privacy principles in the GDPR
0.06	2019-11-13	Marko Kompara	Risk assessment methodology
0.07	2019-11-18	Marko Holbl	Risk assessment matrix
0.08	2019-11-25	Boštjan Kežmah	Technical aspects from guidelines
0.09	2019-12-02	Tamara Bubnjar	Legal aspects from guidelines
0.10	2019-12-06	Marko Kompara	Internal review
0.11	2019-12-11	Tamara Bubnjar	Internal review
0.12	2019-12-15	Marko Holbl	Internal review
0.13	2019-12-20	Marko Kompara	Update with the latest information (questionnaire)
0.2	2019-12-23	Boštjan Kežmah	Review ready version
0.21	2020-01-05	Marko Kompara, Tamara Bubnjar, Marko Holbl	Addressed high-level reviewer (GUF)
0.22	2020-01-18	Marko Kompara, Tamara Bubnjar, Marko Holbl	Addressed reviewer comments (DTU)
0.23	2020-01-20	Marko Kompara, Tamara Bubnjar, Marko Holbl	Addressed reviewer comments (UCY)
0.24	2020-01-23	Pasquale Annicchino	Comments and updated based on the draft

0.3	2020-01-24	Boštjan Kežmah	Revised version
0.31	2020-01-30	Boštjan Kežmah, Marko Kompara, Marko Holbl	Addressed high-level reviewer (GUF)
1.0	2020-01-30	Boštjan Kežmah	Final version

List of Contents

1 Introduction 1
2 How to Use These Guidelines 5
3 Purpose of Data Protection Impact Assessment 7
3.1 Criteria for Carrying Out GDPR Data Protection Impact Assessments 7
3.2 Compliance with Approved Codes of Conduct and the Opinion of Individuals or Their Representatives 11
4 Protection of Personal Data 12
4.1 Data Protection Impact Assessment 12
4.2 Privacy Principles in GDPR 14
4.2.1 Choice and Consent 17
4.2.2 Determination of Lawful Purpose and Limitation of Use 18
4.2.3 The Life Cycle of Personal and Sensitive Information 18
4.2.4 Punctuality and Quality 20
4.2.5 Openness, Transparency and Informing 20
4.2.6 Participation of Individuals 22
4.2.7 Responsibility 22
4.2.8 Security Measures 23
4.2.9 Monitoring, Measuring and Reporting 24
4.2.10 Prevention of Damage 25
4.2.11 Supplier / Third Party Management 26
4.2.12 Management of Incidents 27
4.2.13 Built-in Security and Privacy 29
4.2.14 Free Movement of Information and Legal Restriction 29
5 Risk Assessment Methodology 31
5.1 The Basis for Identifying Potential Sources and Consequences of Risks 31
5.2 Risk Identification 33
5.3 Risk Criteria 35
5.3.1 Assessment of Relevance and Proportionality of Personal Data Processing 37
5.3.2 Assessment of the Risks to Individuals' Rights and Freedoms 38
5.3.3 Analysis of the Risk Assessment of Individuals' Rights and Freedoms 44
6 The Opinion of the Data Protection Officer 46

7 Self – assessment 47
8 Member States Special Requirements 49
9 Conclusion 51
10 References 52

List of Figures

Figure 1: Guidance workflow 5
Figure 2: Activities within the risk management process for the purposes of analysing the impact on privacy 33
Figure 3: Use of biometrics for access control in some Member States 49
Figure 4: Minimum age for consent under the GDPR 50

List of Tables

Table 1: Assessment of criteria for mandatory DPIA implementation 10
Table 2: Decision to implement DPIA 10
Table 3: ISACA privacy principles mapped to other important principles 14
Table 4: ISACA privacy principles in GDPR 17
Table 5: Threat matrix 36
Table 6: Matrix for assessing the relevance and proportionality of personal data 37
Table 7: Legend of compliance rates 37
Table 8: Risk assessment 44
Table 9: Risk group overview by risk group 45
Table 10: Self – assessment 48

List of Acronyms

AICPA	American Institute of Certified Public Accountants
APEC	Asia-Pacific Economic Cooperation
EC	European Commission
EU	European Union
CICA	Canadian Institute of Chartered Accountants
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDPB	European Data Protection Board
GAPP	Generally Accepted Privacy Principles
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
PET	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
RFID	Radio Frequency IDentification
WP29	The Article 29 Working Party of the Directive 95/46 / EC is a group that provides expert opinions to the European Commission in the field of personal data protection and is composed of representatives of national data protection authorities from all EU Member States.

Glossary of Terms

Personal data: any information relating to an identified or identifiable natural person (i.e. data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Subprocessor: is a third party data processor who has or potentially will have access to or process protected data.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Supervisory authority: an independent public authority which is established by a Member State pursuant to Article 51. Namely:

- Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing and to facilitate the free flow of personal data within the Union (‘supervisory authority’).
- Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission.

cross-border processing: means either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State
- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the European Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

1 Introduction

Digitization has increased the volume of data collection and accelerated the flow of information about individuals. As this information can be used for various purposes, the European Union has adopted the General Data Protection Regulation (GDPR) [6] as a new framework superseding Data Protection Directive 95/46/EC. As the GDPR is a regulation, not a directive, it is directly binding and applicable, though it provides flexibility for certain aspects to be adjusted by individual EU Member States.

Contrary to directives that bind EU Member States to the result they must achieve, leaving national authorities the choice of form and method (in practice, supplementing existing or adopting new legislation), the regulation is generally applicable and directly binding for all EU member states.

The digitalization of almost every aspect of daily life and the use of the Internet in both private and business environments have dramatically increased data collection and accelerated the flow of information about individuals. As this vast amount of data can be used for various legitimate as well as illegal purposes, the EU authorities have, after years of negotiation, agreed on a single regulation that will strengthen the rights of individuals across the EU and ensure uniform and coordinated action across Member States.

The ultimate goal of the EU is to create a single European digital market that will not be hampered by the regulatory specificities of individual Member States. The regulation also extends the protection of individuals to foreign companies doing business in the EU and collecting information on European citizens.

Considering all the requirements set forth by the GDPR, it challenges businesses to fulfil the requirements to ensure compliance. The requirements are sometimes vague or too open and therefore subject to interpretation. This is where businesses struggle with their compliance endeavours.

To support businesses as data controllers and as a tool for the development of CyberSec4Europe deliverables, we have assembled privacy guidelines for the development of new information services. Currently one can find opinions and GDPR guidelines scattered over many sources, leaving data controllers with a lot of work to assemble knowledge in a central knowledge base.

This document combines and summarizes known guidelines and opinions in the form of an actionable to-do list, supported by integrated checklists and concrete guidelines with explanations. It presents a baseline to perform data protection impact analysis when needed or required by the regulation.

This document does not replace the need to understand GDPR requirements. It is a combined framework for privacy professionals including Asia-Pacific Economic Cooperation Privacy Guidelines [1], Generally Accepted Privacy Principles from Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA) [2], ISACA Privacy Principles [3] and ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework [4] in a single and transparent framework for supporting day-to-day activities.

Under the GDPR, data controllers and processors must implement “appropriate technical and organisational measures” to secure and ensure the privacy of the personal data they process. The GDPR,

however, does not provide any specific direction on what these measures should be. ISO/IEC 27701:2019 [7] is a recent data privacy extension to ISO/IEC 27001 [8] and ISO/IEC 27002 [9]. ISO/IEC 27701 provides requirements and helps companies manage privacy risks related to personal data. The added purpose of ISO/IEC 27701 is the inclusion of privacy concepts and, in particular, the incorporation of many articles from the GDPR into the ISO framework. Here it is important to mention that privacy principles that are discussed in Chapter 4.1 (Table 4) are the same in ISO/IEC 27701 as they are in ISO/IEC 29100. In fact, ISO/IEC 27701 provides a mapping of these principles to the sections of the standard, where they are addressed.

ISO/IEC 27701 specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving a privacy information management system. ISO/IEC 27701 standard is broad, allowing it wider application, i.e. organisations can use it to comply with different privacy legislation/requirements. However, it does contain an annexe that maps its requirements and controls to the GDPR's requirements. Ultimately organizations can use ISO/IEC 27001 and ISO/IEC 27701 certification to show to stakeholders and regulators that effective systems are in place to support compliance to GDPR and/or other privacy-related legislation.

While ISO/IEC 27701 is an important step forward in an effort to check and show compliance with the GDPR, it is still, unfortunately, a large and complicated document (especially together with ISO/IEC 27001 and ISO/IEC 27002). This document aims to be a simpler guideline to GDPR compliance. Since the document was designed bottom-up from the GDPR and its accompanying guidelines, the structure closely follows GDPR required planning stages and responsibilities and is therefore suitable for businesses that don't closely follow the ISO 27000 family of standards. The methodology also allows controllers to analyse the requirements for processing personal information before actually implementing the complete ISO 27000 family management process. It is primarily targeted at small and medium organizations, with personnel restrictions and organizations that are using guidelines, best practices and standards other than the ISO 27000 family, e.g. COBIT, ITIL and similar. Since these guidelines are implementation-oriented, they can be used as additional best practice guidance and control list to be used with the ISO 27701.

The main benefit of using an ISO/IEC 27701 over these guidelines is the possibility of certification. This process represents an additional cost that smaller organizations might not be willing to take on, while these guidelines are concise and freely accessible without any cost.

When processing personal data there are nine GDPR principles one should be aware of: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Therefore, this methodology expands basic CIA triad that the ISO 27000 family is based on, with additional dimensions specific to privacy and GDPR compliance, making it more suitable to privacy-oriented endeavours.

The essential changes to the new personal data protection framework in Europe are reflected in the basic principles of GDPR. Legal principles of this kind are important criteria that guide the substantive definition of legal rules and how they are enforced. Personal data must be collected, processed and used lawfully (based on one of the foreseen legal bases), in a fair and transparent manner (in relation to the data subject).

They may only be collected for specified, explicit and legitimate purposes (the so-called purpose limitation[1]), which means that the collected personal data may not be processed for other purposes for which they were not obtained (most often for marketing purposes) or processed in a manner incompatible with the purposes for which they were collected.

The minimum data principle restricts all organizations from collecting personal information in such a way that if the data is not necessary to achieve the goal, it is not appropriate to collect it (the online store does not need to collect the birthday of a customer who is not subject to the age limit of purchase). This principle also requires organizations to use less sensitive information than those whose nature or misuse carries more weight (pseudonyms are better than person's full name) and that the data is only available to those persons in the organization who actually need it.

The principle of accuracy is the obligation to check the accuracy and to keep it up to date.

The principle of storage restriction states that personal data are only stored for as long as is necessary for the purposes for which the personal data are processed.

Integrity and confidentiality impose an obligation to process in a way that ensures adequate security of personal data, including protection against unauthorized or lawful processing.

The most important principle, however, is the principle of accountability, which requires management organizations to comply with the fundamental principles and the ability to demonstrate the compliance of the processing with the fundamental principles.

Controllers and processors should, inter alia, achieve this through the implementation of appropriate technical and organizational measures to ensure compliance. These measures may include, are not limited to, internal rules on the protection of personal data and additional training of employees, internal audits of processing activities, etc. Other possible measures may include the minimization of personal data collection, pseudonymisation, transparency, allowing individuals to monitor processing and establishment, and continuous upgrading of security measures. Privacy Enhancing Technologies or PETs are closely linked with the concept of privacy by design, which is required under the GDPR and can help achieve all the mentioned security measures.

As our understanding of privacy requirements progresses, guidelines and opinions change. Therefore, this document should be a live document, with continuous updates as new official guidelines are published and the community reaches new understandings regarding specific privacy requirements.

Specifically, at the time this document went into the final approval stages, European Data Protection Board adopted Guidelines 4/2019 on Article 25 Data Protection by Design and by Default and Guidelines 2/2019 on the processing of personal data under Article 6 paragraph 1(b) of the GDPR in the context of the provision of online services to data subjects were in public consultation. Consequently, further development of this combined framework is essential for its sustainable use.

[1] Article 5 paragraph 1(b) of the GDPR.

The remainder of this deliverable is structured as follows. The first section after the introduction is a short presentation on how these guidelines should be used to help in assessing whether the Data Protection Impact Analysis should be performed and how to actually perform it. The document is also very useful for more generic GDPR compliance questions anybody might have as the Data Protection Impact Analysis also includes prevention of risk associated with non-compliance with the GDPR. Chapter 3 describes the purpose of the Data Protection Impact Analysis and when it should be performed based on the various actions an organization has taken, the personal data it processes and how the data is processed. The next section describes the Data Protection Impact Analysis is some more detail and includes the presentation of all the privacy principles included in the GDPR together with some examples on how these should be understood or realised. Chapter 5 is about risk assessment. It starts with some more general information about how the risks are perceived in the GDPR and is followed with how to identify risks to individuals' rights and freedoms and evaluate the risks' potential for harm. This section also contains a table of possible risks. The table can be used to asses the risks in any organization. The section concludes with another table, designed to help organizations analyse the risk assessments they have performed. Chapter 6 discusses the role of the Data Protection Officer, while the next chapter proposes a self-assessment template that organizations could use, although this step is not required by the GDPR. The second to last chapter introduces some of the differences between Member States that have occurred due to some of the freedom the Regulation permits Member States in detailing their privacy regulations. Chapter 9 concludes this document.

2 How to Use These Guidelines

Users of this guideline should follow the structure of this document as depicted in Figure 1. The goal of the first phase is to identify whether the data processor or controller needs to prepare Data Protection Impact Analysis (DPIA) for compliance reasons or plans to prepare DPIA voluntarily.

Following that decision, the process continues with a collection of data types and data processing activities with analysis regarding privacy.

After the analysis is complete, consultation with the Data Protection Officer (DPO) is mandatory.

Finally, the completion of the self-assessment is recommended, though not required for compliance reasons.

During the use of this document, users will encounter fields where they should upgrade and document their decisions for compliance reasons. These fields are marked as:

Fields intended for individual explanations for compliance reasons.

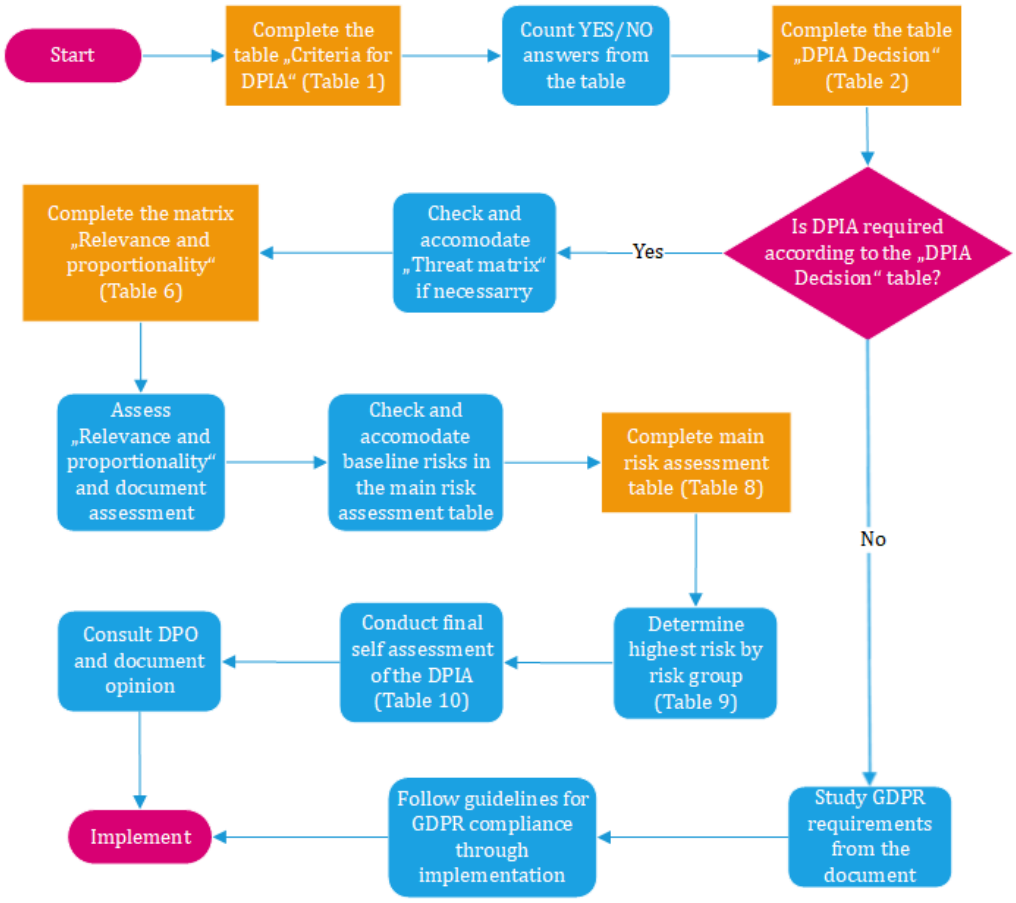

Figure 1: Guidance workflow

While filling those fields is mandatory, the document itself is not meant as a final template, therefore users are free to change an upgrade these guidelines as needed. Users of the guidelines are especially welcome to change and add identified threats in the threat analysis baseline.

3 Purpose of Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process that helps organisations identify and minimise risks that result from data processing. DPIAs are usually undertaken when introducing new data processing processes, systems or technologies. Regular DPIAs supports the GDPR's accountability principle, helping organisations demonstrate compliance. Conducting a DPIA can also help increase awareness of privacy and data protection issues within an organisation. An impact assessment should include measures, safeguards and mechanisms designed to mitigate risk, ensure the protection of personal data and demonstrate compliance with the GDPR.

DPIA is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular, because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

A data protection impact assessment may indicate that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons. If the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies or costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular, the measures envisaged mitigating the risk to the rights and freedoms of natural persons.

3.1 Criteria for Carrying Out GDPR Data Protection Impact Assessments

A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the

processing of personal data (by assessing them and determining the measures to address them). DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR but also to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR. In other words, a DPIA is a process for building and demonstrating compliance.

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35 paragraph 1), illustrated by Article 35 paragraph 3 and complemented by Article 35 paragraph 4. It is particularly relevant when a new data processing technology is being introduced.

The more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. As a rule of thumb, a processing operation meeting less than two criteria may not require a DPIA due to the lower level of risk, and processing operations which meet at least two of these criteria will require a DPIA.

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing (Table 1).

Publishing a DPIA is not a legal requirement of the GDPR. It is left upon the controller´s decision. However, data controllers should consider publishing their DPIA, or perhaps part of their DPIA results. The purpose of such a process would be to help foster trust in the controller's processing operations and demonstrate accountability and transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA. The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. It could even consist of just a summary of the DPIA's main findings. Moreover, when a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36 paragraph 1). As part of this, the DPIA must be provided (Article 36 paragraph 3(e)).

Nr.	Factor	Requires DPIA (YES/NO)	Explanation
Basic conditions[2]			
1	An impact assessment has not yet been carried out		
2	The impact assessment was not carried out for a long time since the first personal data processing		

[2] Based on Recital (89) of the GDPR.

3	A substantial change in processing that may affect compliance		
4	Change of regulations or guidelines that may affect the DPIA or GDPR compliance		
The risk associated with the type of processing[3] (always if at least 2 conditions are met)			
5	It is likely that the processing of personal data will pose a high risk		
6	Processing involves the use of new technologies		
7	Processing involves evaluation or scoring, including profile formation and prediction (e.g., personal taste, interest, health, location, movement)		
8	Automated decision making has legal or similarly significant effects		
9	Processing involves systematic monitoring (e.g observation, monitoring control)		
10	Processing involves sensitive or very personal information (e.g. specific types of data, criminal convictions, misdemeanours)		
11	Datasets are combined (exceeding reasonable expectations of an individual)		
12	Data refers to vulnerable individuals (disproportionate power between the data controller and individuals)		
13	Processing refers to a significant amount of personal data at the regional level		
14	Processing refers to a considerable amount of personal data at the national level		
15	Processing refers to a considerable amount of personal data at the transnational level		
16	Processing can affect a large number of data subjects		

[3] Based on guidelines on data protection impact assessment and the determination of whether "[processing] is likely to present a high risk" for the purposes of Regulation (EU) 2016/679, revised 4 October 2017, p. 8; Recital (91) of the GDPR; Article 35 of the GDPR.

17	Processing impedes or prevents the exercise of the rights of an individual		
18	Processing prevents individuals from using the service or contract		
19	Processing is used to make individual decisions about individuals and includes biometric data		
20	Processing is used to make decisions regarding individuals and includes information on criminal convictions and misdemeanours or related actions		
21	Monitoring of publicly accessible areas on a large scale		
Mandatory performance of the impact assessment[4]			
22	The processing is listed in the list of personal data processing actions that are subject to the requirement to carry out an impact assessment regarding the protection of personal data[3]		

Table 1: Assessment of criteria for mandatory DPIA implementation

The data protection impact assessment should be carried out when at least one of the basic criteria and at least one of the subsets of criteria are true (Table 2).

Number	Criteria	DPIA Implementation Decision (YES / NO)	Explanation
1	Mandatory performance criteria are met to perform DPIA		
2	We perform DPIA voluntarily		

Table 2: Decision to implement DPIA

The performance of a data protection impact assessment is optional if it involves the processing of personal data of patients or clients by an individual doctor, another healthcare professional or a lawyer[5].

Likewise, the data protection impact assessment is optional if the processing is listed in the list of types of processing actions that are not subject to the data protection impact requirement[6].

[4] Based on Article 35 paragraph 4 of the GDPR.
[5] Recital (91) of the GDPR.

An impact assessment is also not required if the processing was approved before May 2018 and was unchanged since then or if there is a legal basis for processing. If it is not clear whether DPIA implementation is mandatory, then implement it [5].

3.2 Compliance with Approved Codes of Conduct and the Opinion of Individuals or Their Representatives

Explain whether codes of conduct affect impact assessment as defined in Article 35 paragraph 8 of the GDPR.

The data controllers are expected to comply with Article 35 paragraph 9 of the GDPR, where appropriate, and get the opinion of data subjects.

Explain whether you plan to get the opinion of data subjects and how this will be done.

[6] Article 35 paragraph 5 of the GDPR.

4 Protection of Personal Data

GDPR radically changed the regulation of personal data protection; it conferred more rights to individuals and imposed more obligations on companies collecting and processing personal data. The regulation is applicable not only to information service providers established in the EU but also to those who have their place of business outside the EU and process information about individuals located in the EU. Personal data has to be processed lawfully and in a fair and transparent way. Collecting personal data can be done only for a particular, explicit and lawful purpose. The data has to be appropriate, relevant and limited to the purposes for which it is being processed. Furthermore, it has to coincide with the facts and has to be up-to-date. Moreover, it can be stored no longer than the purpose allows it. Finally, the data must be protected with appropriate measures against unauthorised and unlawful processing as well as accidental loss, destruction and damage.

4.1 Data Protection Impact Assessment

DPIAs are a useful way for data controllers to implement data processing systems that comply with the GDPR and can be mandatory for some types of processing. They are scalable and can take different forms, but the GDPR sets out the basic requirements of an effective DPIA. Data controllers should see the carrying out of a DPIA as a useful and positive activity that aids legal compliance.

The DPIA is a key part of complying with the Regulation where high-risk data processing is planned or is taking place. This means that data controllers should use the criteria set out in this document to determine whether or not a DPIA has to be carried out. Internal data controller policy could extend this list beyond the GDPR's legal requirements. This should result in greater trust and confidence of data subjects and other data controllers.

Article 35 paragraph 7 requires that the data protection impact assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1 (where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data)
- the measures envisaged addressing the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the

GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

ISACA PRIVACY PRINCIPLES[7]	GDPR	ISO/IEC 29100:2011	APEC	GAPP
1. Choice and consent	Notice & consent	Consent and choice	Choice	Choice and consent
2. Determination of lawful purpose and limitation of use	Legitimate purpose and automated decision making	Purpose legitimacy and specification, and use, retention and disclosure limitation	Use of personal information	Use, retention and disposal
3. The life cycle of personal and sensitive information	Privacy by Design, DPIAs, Data Subject Participation & Safeguards	Collection limitation, and Data minimization	Collection limitations	Collection
4. Punctuality and quality	Data rectification and data quality	Accuracy and quality	The integrity of personal information	Quality
5. Openness, transparency and information	Transparency and data subject rights	Openness, transparency and notice	N/A	N/A
6. Participation of individuals	Data subject access	Individual participation and access	Access and correction	Access
7. Responsibility	Data Processing, Data Protection Officers & Controllers	Accountability	Accountability	Management
8. Security measures	Security Safeguards Throughout Data Lifecycle	Information security	Security safeguards	Security for privacy
9. Monitoring, measuring and reporting	Processing, right to be forgotten and data portability records/ reports	Privacy Compliance	N/A	Monitoring and enforcement
10. Prevention of damage	Lawfulness, Data Subject Access, Portability & DPIAs	N/A	Damage prevention	N/A
11. Supplier / third party management	Management of processors	N/A	N/A	Disclosure to third parties
12. Management of incidents	Violation management and notification	N/A	N/A	N/A

13. Built-in security and privacy	Controller Responsibilities, Automated Decision-Making & Data Protection by Default	N/A	N/A	N/A
14. Free movement of information and legal restriction	Data Subject Rights, Lawfulness, Data Transfers, Binding Corporate Rules	N/A	N/A	N/A

Table 3: ISACA privacy principles mapped to other important principles

4.2 Privacy Principles in GDPR

This table (Table 4) provides readers with information about the GDPR, the benefits of using the ISACA privacy principles to perform GDPR-required data protection impact assessments (DPIA), which are a specific type of Privacy Impact Assessment (PIA), and how to accomplish GDPR DPIAs using the privacy principles.

The GDPR requires each data controller and data processor to perform DPIAs under certain specific circumstances. These go beyond traditional PIAs, which focus on the risk that is primarily to the enterprise itself. The DPIA process is designed to:

- describe the processing
- assess the necessity and proportionality of the processing
- determine compliance with the GDPR requirements
- help manage the risk to the rights and freedoms of natural persons that result from processing personal data and determine appropriate measures to address this risk. DPIAs also support accountability by helping data controllers and data processors not only to comply with all the requirements of the GDPR but also to demonstrate due diligence that the enterprise is taking appropriate actions to ensure full compliance on an ongoing basis.

In addition to the GDPR, most organizations must also ensure compliance with multiple other legal requirements for personal data by performing PIAs. Including the other personal data protection requirements in the DPIA process for the GDPR is the most efficient and beneficial approach for an enterprise, regarding resources and time. Enterprises can use the ISACA privacy principles as the framework for their DPIA by following these steps:

- group the GDPR and other requirements within each of the 14 ISACA privacy principles (Table 4)
- address the GDPR requirements through questions that apply to the DPIA
- adjust the questions so that they apply to similar requirements from the other data protection legal obligations
- address the other requirements through the adjusted questions.

This consolidated approach accomplishes the GDPR DPIA and the required PIAs for the other privacy principles and standards, eliminating the need to perform separate PIAs.

ISACA privacy principles [3]	**Relevant articles in GDPR**
1. CHOICE AND CONSENT	Article 6: Lawfulness of processing Article 7: Conditions for consent Article 8: Conditions applicable to child's consent in relation to information society services
2. DETERMINATION OF LAWFUL PURPOSE AND LIMITATION OF USE	Article 5: Principles relating to the processing of personal data Article 6: Lawfulness of processing Article 10: Processing of personal data relating to criminal convictions and offences Article 22: Automated individual decision-making, including profiling Article 39: Tasks of the data protection officer
3. THE LIFE CYCLE OF PERSONAL AND SENSITIVE INFORMATION	Article 5: Principles relating to the processing of personal data Article 6: Lawfulness of processing Article 9: Processing of special categories of personal data Article 21: Right to object Article 25: Data protection by design and by default Article 35: Data protection impact assessment Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
4. PUNCTUALITY AND QUALITY	Article 5: Principles relating to the processing of personal data Article 16: Right to rectification
5. OPENNESS, TRANSPARENCY AND INFORMATION	Article 5: Principles relating to the processing of personal data Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject Article 13: Information to be provided where personal data are collected from the data subject Article 14: Information to be provided where personal data have not been obtained from the data subject Article 15: Right of access by the data Article 21: Right to object
6. PARTICIPATION OF INDIVIDUALS	Article 7: Conditions for consent Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject Article 14: Information to be provided where personal data have not been obtained from the data subject Article 15: Right of access by the data Article 16: Right to rectification Article 17: Right to erasure (‘right to be forgotten’) Article 18: Right to restriction of processing Article 20: Right to data portability Article 21: Right to object

	Article 22: Automated individual decision-making, including profiling Article 26: Joint controllers Article 38: Position of the data protection officer
7. RESPONSIBILITY	Article 5: Principles relating to the processing of personal data Article 6: Lawfulness of processing Article 14: Information to be provided where personal data have not been obtained from the data subject Article 24: Responsibility of the controller Article 27: Representatives of controllers or processors not established in the Union Article 32: Security of processing Article 36: Prior consultation Article 37: Designation of the data protection officer Article 38: Position of the data protection officer Article 39: Tasks of the data protection officer
8. SECURITY MEASURES	Article 5: Principles relating to the processing of personal data Article 6: Lawfulness of processing Article 24: Responsibility of the controller Article 32: Security of processing Article 46: Transfers subject to appropriate safeguards
9. MONITORING, MEASURING AND REPORTING	Article 17: Right to erasure (‘right to be forgotten’) Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 20: Right to data portability Article 30: Records of processing activities Article 33: Notification of a personal data breach to the supervisory authority Article 34: Communication of a personal data breach to the data subject Article 35: Data protection impact assessment Article 37: Designation of the data protection officer Article 39: Tasks of the data protection officer Article 47: Binding corporate rules
10. PREVENTION OF DAMAGE	Article 6: Lawfulness of processing Article 15: Right of access by the data Article 20: Right to data portability Article 22: Automated individual decision-making, including profiling Article 35: Data protection impact assessment Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes Article 91: Existing data protection rules of churches and religious associations
11. SUPPLIER / THIRD PARTY MANAGEMENT	Article 28: Processor Article 29: Processing under the authority of the controller or processor Article 32: Security of processing

12. MANAGEMENT OF INCIDENTS	Article 33: Notification of a personal data breach to the supervisory authority Article 34: Communication of a personal data breach to the data subject
13. BUILT-IN SECURITY AND PRIVACY	Article 22: Automated individual decision-making, including profiling Article 24: Responsibility of the controller Article 25: Data protection by design and by default
14. FREE MOVEMENT OF INFORMATION AND LEGAL RESTRICTION	Article 6: Lawfulness of processing Article 21: Right to object Article 44: General principle for transfers Article 45: Transfers on the basis of an adequacy decision Article 46: Transfers subject to appropriate safeguards Article 47: Binding corporate rules Article 48: Transfers or disclosures not authorised by Union law Article 49: Derogations for specific situations

Table 4: ISACA privacy principles in GDPR

4.2.1 Choice and Consent

When data controllers or processors collect personal information from individuals, they should describe the options that the individual has and obtain appropriate consent appropriately in the context of the particular case.

In accordance with the GDPR, the following should be considered:

- the existence of a documented and implemented privacy policy and support procedures that provide choices where appropriate
- consents obtained must be properly documented and maintained to the extent that the data controller collects information from individuals under the age of 16, documented policies and processes must be in place to obtain parental responsibility for those individuals.

Consent is valid if it is:

- **Provable**: consent is demonstrable, allowing the data controller to express it at any time at the request of the supervisory authority.
- **Voluntary**: consent is voluntary which:
    - provides true choice and control
    - does not arise from the disproportionate power relationship between the controller and the individual (e.g. employment, public authority, etc.)
    - is not a condition for the conclusion of a contract
    - can be withdrawn by the individual at any time
    - does not have adverse effects on the individual if they do not give it or withdraw it.
- **Specific**: the specific consent is given for a specific purpose.
- **Informed**: consent is informed, when it clearly states:
    - who is the data controller
    - for what purpose the data will be processed

- that the individual may withdraw the consent at any time
- have the right not to be subject to a decision based solely on automated processing, including the creation of profiles
- the potential risks of transferring personal data to a third country or an international organization.

- **Unambiguous:** consent is given by a clear affirmative action and must not be presumed.

EXAMPLE:

A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given. [5]

4.2.2 Determination of Lawful Purpose and Limitation of Use

This principle requires from data controllers/data processors to clearly describe to data subjects and data protection authorities, as appropriate, the purposes for collecting information and then limit information processing to those purposes.

In accordance with the GDPR, the following should be considered:

- existence of a documented and implemented privacy policy and support procedures for obtaining consent to collect and process only personal data that are necessary, relevant and limited for the purposes for which they were collected and will be processed
- the introduction of mechanisms and controls to ensure that the intended further processing will be reviewed, and appropriate measures are taken prior to such use (such as obtaining consent and ensuring legal compliance)
- the specificity and documentation of the cases in which the right of objection cannot be invoked and the appropriate supportive procedures applicable in those cases are put in place.

EXAMPLE:

A data subject provides their postal code to see if a particular service provider operates in their area. This can be regarded as necessary processing to take steps at the request of the data subject prior to entering into a contract pursuant to Article 6 paragraph 1(b).[5]

4.2.3 The Life Cycle of Personal and Sensitive Information

Controllers and processors must restrict the collection and all processing of information to certain documented purposes and then ensure that the processing of information is consistent with those specified purposes throughout the life cycle of the processing of personal data, including retention and destruction. If the information is subject to further processing at any point in the life cycle, then new consent must be obtained and / or it must be already compliant with the intent of the original processing.

In accordance with the GDPR, the following should be considered:

- the existence of a documented and implemented policy and support procedures to ensure that personal data remain in storage only for such time as is strictly necessary to achieve the purpose for which it was collected, in support of a legal and potential public interest, scientific or historical purpose
- established methods and technologies that allow individuals to request removal from the controller or processor processes that use personal information for direct advertising purposes
- existence of a documented and implemented privacy policy and support procedures requiring the implementation of appropriate technical and organizational or process measures that ensure that only the data required for each specific purpose will be processed by default.

For EU personal data processing, data protection by default is particularly relevant for systems which directly interact with users, inside or outside the EU Institutions. Where appropriate, any processing operations shall be limited to what is the absolutely necessary, as regards "the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility" for persons or organisations. This should also be applied to any tracking functions, e.g. in the context of web services or mobile apps.

Personal information security throughout the life cycle involves:

- considering whether it is actually necessary to collect and hold personal information in order to carry out functions or activities
- planning how personal information will be handled by embedding privacy protections into the design of information handling practices
- assessing the risks associated with the collection of personal information due to a new act, practice, change to an existing project or as a part of usual business
- taking appropriate steps and putting into place strategies to protect the personal information that you hold
- destruction or de-identification of personal information when it is no longer needed.

To effectively protect personal information throughout its life cycle, it is necessary to be aware of when and how it is collected and when and how it is stored. As noted above, personal information holdings can be dynamic and change without any necessarily conscious or deliberate action.

Additionally, the life cycle may include the passing of personal information to a third party for storage, processing or destruction.

EXAMPLE:

Access controls ensure that only authorised individuals can read, modify or delete data in the system. Such controls help achieve confidentiality and integrity from a security perspective. Additionally, when an IT system processes personal data, the built-in controls should make sure that users can access only specific data to perform their duties. Access controls can thus help ensure that the use of personal data is

limited to authorised purposes (purpose limitation) and data is protected from unauthorised access and tampering. [5]

4.2.4 Punctuality and Quality

The data controller must, at the request of the data subject, correct inaccurate personal data relating the subject or delete personal data that the individual proves to be no longer necessary for the purposes for which they were collected or otherwise processed, there is no legal basis for their processing, the individual objects to their processing and there are no overriding legitimate reasons for their processing, they were collected or processed unlawfully, they must be deleted to fulfil the legal obligation applicable to the controller, or they have been collected in connection with the provision of information society services by a minor. Data controllers or processors must ensure that information is accurate, complete and up to date in order to reduce the risk of inaccurate information being used for decision making.

The principle of accuracy (and timeliness) dictates that the data being processed must be accurate and up-to-date. Accuracy means that the information is not incorrect or incomplete, and up-to-date means that the latest information is used. Personal data may be accurate but not up to date, which means that data that was otherwise accurate and valid is no longer valid because a more recent piece of information exists.

In accordance with GDPR, the following should be considered:

- the introduction of a mechanism for correcting personal data, where necessary, at all locations where data are stored
- existence of documentation that records or lists all changes to personal data, including the date, time, who changed the data and similar
- an established process that provides individuals with a method for requesting corrections to their wrong personal information.

Personal data should be accurate and kept up to date. In accordance with Article 6 of Directive 95/46/European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, every reasonable step must be taken to ensure that data are kept accurate and up to date, with regard to the purposes for which they were collected or for which they are further processed. Moreover, in light of the GDPR, the public sector subject will have the right to obtain from the competent institutions, without undue delay, the rectification of their personal data which are inaccurate or out of date. Also, Article 16 of the GDPR states that, depending on the purposes for which data were processed, the data subject will have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement [10].

4.2.5 Openness, Transparency and Informing

Controllers or processors must provide clear, accessible and accurate details of their privacy management program, how they process information, and time frame for providing this information.

Articles 13 and 14 of the GDPR set out information which must be provided to the data subject at the commencement phase of the processing cycle. Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:

- a data subject consciously provides to a data controller (e.g. when completing an online form)
- a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:

- third party data controllers
- publicly available sources
- data brokers
- other data subjects[8]

In accordance with GDPR, the following should be considered:

- existence of documented and enforced privacy notices and support procedures and processes for communicating with individuals regarding their rights and information, with a description of the processing in a clear, easily understandable and age-appropriate format
- the existence of a documented and enforced privacy policy and support procedures and processes that provide individuals with information related to processing for any purpose other than those for which the data was originally collected prior to further processing
- existence of a documented and enforced privacy policy and support procedures and processes for informing individuals of the safeguards in use when transferring data to a third country or to another international controller or processor
- at the time the personal data are collected, further information regarding the existence of the portability right must be provided to the user
- in relation to information on the existence of automatic decision-making, including profiling, an individual must receive essential information about the logic involved and its relevance and intended profiling goals for the individual.

EXAMPLE:

Every organisation that maintains a website should publish a privacy statement/notice on the website. A direct link to this privacy statement/notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", "Privacy Policy" or "Data Protection Notice"). Positioning or colour schemes that make a text or linkless noticeable, or hard to find on a webpage, are not considered easily accessible. [5]

[8] Article 29 Working Party Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, last Revised and Adopted on 11 April 2018.

4.2.6 Participation of Individuals

Controllers and processors must guarantee individuals the right of access, portability, access, confirmation, correction and restriction of the processing and deletion of related data, as well as the withdrawal of consent already given. Furthermore, simple methods must be available to exercise these rights.

In accordance with the GDPR, the following should be considered:

- The existence of a documented and enforced privacy policy, supportive procedures and simple processes that allow individuals to withdraw consent at any time, including personal data in partnership with other data controllers, as long as this right is not limited by other legislation.
- Procedures and methods, in partnership with any other joint controller, allow the verified individual to exercise his or her rights to request access, information, correction, deletion or destruction, and restrictions on their personal data in accordance with time requirements, costs and format as specified in the GDPR.
- The introduction of a mechanism allowing the verified individual the opportunity to obtain confirmation as to whether or not personal data concerning the individual are being processed, in which case he shall be able to obtain information on categories, recipients, retention times, deletion rights and complaints, and the possible restrictions on the processing of personal data where practicable, legal notices where the restriction is lifted and data sources where possible.

The controller has to bring details of the right to object under Article 21 paragraph 1 and 2 explicitly to the data subject's attention and present it clearly and separately from other information.

Once the data subject exercises this right, the controller must interrupt (or avoid starting) the profiling process unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject. The controller may also have to erase the relevant personal data.

EXAMPLE:

A local surgery's computer system places an individual into a group that is most likely to get heart disease. This 'profile' is not necessarily inaccurate even if he or she never suffered from heart disease. The profile merely states that he or she is more likely to get it. That may be factually correct as a matter of statistics. Nevertheless, the data subject has the right, taking into account the purpose of the processing, to provide a supplementary statement. In the above scenario, this could be based, for example, on a more advanced medical computer system (and statistical model) factoring in additional data and carrying out more detailed examinations than the one at the local surgery with more limited capabilities. [5]

4.2.7 Responsibility

Controllers or processors are generally required to take actions to demonstrate accountability throughout their workforce for appropriate governance and risk management of the information to which they have responsibilities and to ensure all related activities are performed in compliance with all associated legal requirements.

In accordance with the GDPR, the following should be considered:

- the existence of a documented and enforced privacy policy and support procedures for establishing requirements for the responsibilities of the Data Protection Officer and the activities for which the Data Protection Officer is responsible, together with ensuring that the persons performing the role are appropriately qualified and have adequate knowledge
- the existence of a documented and enforced privacy policy and support procedures to ensure accountability for certain roles within the organization to communicate with individuals when information is not obtained directly from them
- establishment of procedures that ensure accountability for a specific role within the organization for consulting the supervisory authority prior to processing if a privacy impact analysis finds that the processing result is high risk in the absence of risk mitigation measures.

EXAMPLE:

A data broker undertakes to profile of personal data. In line with their Article 13 and 14 obligations, the data broker should inform the individual about the processing, including whether they intend to share the profile with any other organisations. The data broker should also present separately details of the right to object under Article 21 paragraph 1. The data broker shares the profile with another company. This company uses the profile to send the individual direct marketing. The company should inform the individual (Article 14 paragraph 1(c) about the purposes of using this profile, and from what source they obtained the information (Article 14paragraph 2(f). The company must also advise the data subject about their right to object to processing, including profiling, for direct marketing purposes (Article 21 paragraph 2). The data broker and the company should allow the data subject the right to access the information used (Article 15) to correct any erroneous information (Article 16), and in certain circumstances erase the profile or personal data used to create it (Article 17). The data subject should also be given information about their profile, for example in which 'segments' or 'categories' they are placed. If the company uses the profile as part of a solely automated decision-making process with legal or similarly significant effects on the data subject, the company is the controller subject to the Article 22 provisions. (This does not exclude the data broker from Article 22 if the processing meets the relevant threshold.)[5]

4.2.8 Security Measures

Article 32 of the GDPR states that data controller and processor have to provide appropriate technical and organizational measures an appropriate level of risk-based security. Measures to be taken into account:

- state of the art technological developments
- costs of implementation
- nature
- scope
- circumstances
- processing purposes
- risks to the rights and freedoms of individuals

They are taken into account when determining the appropriate level of security given the risks posed by processing, in particular for unintentional or unlawful destruction, losses, changes, unauthorized disclosures or access to personal information that is sent, stored or otherwise processed.

The controller and the processor ensure that any natural person acting under the data controller or processor that has access to personal data, may not process this data unless allowed to do so by the data controller's Union or Member State law.

Data controllers or processors must ensure that adequate security measures are in place for all information within the organization and for the entire life cycle of the information at any location where the information is processed.

In accordance with the GDPR, the following should be considered:

- the existence of a documented and enforced security policy and support procedures to ensure that adequate data protection is in place, including protection against unauthorized or unlawful processing and protection against accidental loss, destruction or damage
- introduced methods and technologies to assess the likelihood of harming the privacy of individuals in the event of unauthorized sharing, unauthorized use, unauthorized or unintentional destruction, loss or alteration, and other access to personal data, and subsequently implemented technical measures and other measures by controllers or processors to ensure a level of security that is appropriate in relation to the detriment such an event would cause to an individual
- the documented procedures and technologies used to ensure the security of information transmitted to a third country or to an international controller or processor.

4.2.9 Monitoring, Measuring and Reporting

Each processor shall keep records of all types of processing activities performed on behalf of the controller, which shall include:

- the name and contact details of the processor or processors and of each controller on whose behalf the processor operates, and, where available, of a representative of the controller or processor, and of the operational programme authorized person
- the types of processing carried out on behalf of each controller
- where appropriate, transfers of the personal data to a third country or international organization, including the identification of that third country or international organization, and, in the case of transfers referred to in the second subparagraph of Article 49 paragraph 1, documentation of appropriate safeguards
- where possible, a general description of the technical and organizational security measures referred to in Article 32 paragraph 1.

The records shall be in writing, including in electronic form.

Controllers or processors must put in place appropriate and consistent monitoring, measurement and reporting capabilities to determine the effectiveness of a program and privacy management tools.

In accordance with the GDPR, the following should be considered:

- the existence of a documented policy and support procedures showing detailed reports and tasks under the responsibility of the Data Protection Officer in order to verify that the controller or processor provides sufficient and continuous training of the staff in privacy and security
- introduction of reporting processes and technologies to provide details to individuals of related deletions or incorrect information
- carrying out processes for reporting the contact details of the Data Protection Officer and breaches of personal data protection to the supervisory authority.

4.2.10 Prevention of Damage

Controllers and processors must have processes and tools in place to identify and document the potential harm to individuals' privacy in the event of misuse or invasion of the information under the responsibility of the controller or processor.

In accordance with the GDPR, the following should be considered:

- that risk prevention policies and support procedures are in place to determine whether data processing is legal in at least the following cases:
    - the individual has given explicit consent
    - processing is necessary to fulfil a contract with an individual
    - processing is required by regulations
    - processing protects the vital interests of the individual
    - processing is necessary in the public interest
    - processing is necessary to achieve the legitimate interests of the controller or processor or third parties
- there are consistent procedures in place to ensure that decisions regarding individuals are not made on the basis of specific types of personal data unless specific safeguards have been put in place
- that there are documented harm prevention policies, support procedures and processes, and tools in place, to ensure that individuals exercising their rights in connection with the use of their personal data and requesting copies of personal data and exercising other GDPR rights are not adversely affected. to the rights and freedoms of others.

The term 'right' does not mean that Article 22 paragraph 1 of the GDPR applies only where the individual to whom personal data relates, actively asserts the right. Article 22 paragraph 1 of the GDPR establishes a general prohibition on decisions based solely on automated processing. This prohibition shall apply whether or not the data subject takes steps to process their own personal data.

This interpretation supports the idea that the data subject has control over their personal data, which is in accordance with the basic principles of the GDPR. If Article 22 is interpreted as prohibition rather than a right to be exercised, that is, individuals are automatically protected against the potential effects of such treatment.

With any processing that could pose a high risk to the individuals to whom personal data refers to, the controller must carry out a data protection impact assessment. In addition, addressing any other processing risks may be an impact assessment related to Data protection is particularly useful for controllers who are not sure whether their proposed data activities fall within the definition in Article 22 paragraph 1 and, if permitted by the defined exception, which safeguards must be implemented.

The controller should identify and record in the context of the data protection impact assessment the degree of any personal intervention in the decision-making process and the stage at which performs.

EXAMPLE:

Some insurance companies offer insurance rates and services based on the behaviour of the individual while driving. The elements taken into account in these cases could include distance travelled, driving time and the trip done, as well as predictions based on other data collected by the sensors into a (smart) car. The data collected is used to create profiles to identify inappropriate driving behaviour (such as fast acceleration, sudden braking and speeding). To better understand the driver's behaviour, this information can be cross-referenced with other sources (e.g. weather, traffic, type of road). The controller must ensure that they have a legal basis for such processing. In addition, it must provide the data subject with information about the data collected and, if it is appropriate for the existence of automated decision-making referred to in Article 22 paragraph 1 and paragraph 4, the reasons therefor, and the importance and anticipated consequences of such processing. [5]

4.2.11 Supplier / Third Party Management

Controllers or processors must put in place and implement appropriate policies, processes and tools to provide for ongoing oversight of the third parties to which they entrust any type of access to information for which the controller or processor is responsible.

In accordance with the GDPR, the following should be considered:

- that there are documented third party or vendor management policies and support procedures in place to ensure that the organization does not use third parties or suppliers if they do not provide sufficient guarantees and verifiable evidence that they have put in place adequate technical, physical and organizational measures and controls that support the rights of individuals, and contractually undertake to notify the organization whenever changes occur, including hiring or terminating the involvement of other processors
- that there are documented procedures detailing the activities to be performed by third parties or suppliers as processors and the evidence that they must collect if they include other processors in the processing to perform certain processing activities for which they have been hired by organizations and involve a third party or a supplier, and with the assurance that such sub-processing includes the same requirements as those agreed with the contract manager
- that there are documented third party or vendor management policies that set out the procedures to be followed by the organization to ensure that staff operating within the mandate of the organization and third parties or suppliers who have access to personal information follow all privacy policies; and procedures and instructions to be provided by the organization and the third

party or supplier for which the staff work, and the relevant rules and requirements of the EU or Member State.

The data controller can, therefore, trust data to processors that provide sufficient guarantees for the implementation of appropriate technical and organizational measures[9]. Controllers should consider at least the following elements when determining whether given guarantees are sufficient:

- processor references
- the presence and confidence that the processor enjoys on the market
- provision of appropriate Terms of Service

Namely, the controller must retain control over entities that have contact with personal data from the controller's data sets. Chaining processing can mean loss of control and any entity in the chain may commit a misuse of personal information. That's why it is crucial that the controller can make decisions, with whom the processors will work and when it will allow subprocessors. General Regulation stipulates that the processor must not employ the second processor without the prior special or general written permission of the controller. Consent of each subprocessor, that the controller may issue the processor to which it trusted enough to hire only trusted one's subprocessors and in accordance with the General Regulation may be duly regulated by mutual agreement relationship. In the case of generally written permissions, the latter must be handled by the controller and processors have to notify controllers of any intended changes regarding the employment of additional processors or their replacement, thereby giving the controller possibility to oppose these changes. The controller may not agree that the subprocessor would transfer personal information to third countries, does not have the confidence of the controller or there may be any third reason why the controller does not allow the use of the services of a particular subprocessor.

EXAMPLE:

The merchant hires an IT loyalty club maintenance company, and the IT company does not store the loyalty club data on their servers but continue to hire services from a hosting provider. In large-scale solutions, the chains can also include dozens of processors and their sub-processors. [5]

4.2.12 Management of Incidents

Controllers or processors must put in place policies, procedures and methods to prevent, quickly identify and respond to and effectively reduce the consequences of privacy breaches.

Violation of personal data security, as defined in Articles 33 and 34 of the Regulation includes incidents resulting in unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data. The violation may be committed inadvertently (e.g. by negligence) or may be intentional or unintentional. Generally, a breach constitutes a security incident that threatens the confidentiality, integrity and accessibility of personal data.

[9] Some informal tools and alliances already exist, e.g. Privacy Pact, https://privacypact.com/.

In practice, breaches of personal data security may include:

- access by an unauthorized person
- providing personal information to the wrong address
- loss or theft of computer equipment containing personal information
- unauthorized destruction of personal data
- change of personal data without the necessary permission
- loss of access to personal data (e.g. loss of password or loss of equipment that enables decryption)
- unauthorized installation of an encryption program that prevents access to data (e.g. ransomware).

In accordance with the GDPR, the following should be considered:

- that there are documented privacy breach policies and support procedures that include requirements for timely notification of the appropriate oversight authorities of the data breach and any possible reasons for the delay when reporting it
- that there are documented procedures and support tools for informing individuals without delay and no later than 72 hours from the detection of an incident, in the event that an assessment of the damage or risk involved would endanger the rights and freedoms of individuals
- that there are processes and mechanisms in place to document and report on any breach of personal data, including facts related to the breach, potential consequences for individuals, and mitigation measures taken by the organization.

The GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become “aware” of a breach. WP29 considers that a controller should be regarded as having become “aware” when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised [5].

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. The fact that the notification was made without undue delay should be established taking into account, in particular, the nature and gravity of the breach and its consequences and adverse effects for the data subjects. This puts an obligation on the controller to ensure that they will be “aware” of any breaches in a timely manner so that they can take appropriate action.

When exactly, a controller can be considered to have become “aware” of a particular breach will depend on the circumstances of a specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas, in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine

whether personal data have indeed been breached and if so, to take remedial action and notify relevant parties if required.[10]

EXAMPLE:

The controller uses a company that provides information services (processor) to use the services of storing and archiving information about its customers. The processor detects an intrusion into its information system and unauthorized access to the databases of its client - the controller. The processor shall immediately notify the incident to the controller, who shall then notify the Information Commissioner thereof. [5]

4.2.13 Built-in Security and Privacy

Controllers and processors must document the organization's privacy strategy and the support policies and procedures by which the company conducts business activities with built-in security and privacy protections.

In accordance with the GDPR, the following should be considered:

- that there are documented procedures and supportive technologies in place to build security and privacy safeguards throughout the lifecycle of automated decision-making processes involving personal data
- that mechanisms are in place to allow individuals to express their views on their records, regarding decisions made based on that data, and to challenge the decisions made
- that there are documented and enforced policies and support procedures for assessing the risk associated with the nature, extent, context and purposes of the processing of personal data and the associated likelihood and severity of harm to individuals.

EXAMPLE:

In the case of a loss of a USB key with unencrypted personal data, it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be reported as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost. [5]

4.2.14 Free Movement of Information and Legal Restriction

Controllers and processors must document the philosophy of privacy and support policies and procedures by which an organization protects the personal information it transmits across borders to support business activities.

[10] Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, last Revised and Adopted on 6 February 2018.

Data Protection Impact Assessments, as defined in Article 35 of the GDPR, are one of the key concepts under the responsibility principle. Impact assessments related to the protection of personal data are a tool for identifying, analysing and reducing the risks of unlawful handling of personal data that may occur in a particular project, system or use of technology. Controllers perform an impact assessment when it is possible that a particular type of processing would pose a high risk to individuals' rights and freedoms.

It is advisable for controllers to carry out impact assessments for major projects involving the processing of personal data.

The impact assessment should include:

- a systematic description of the actions and purposes of the processing and, where appropriate, of the legitimate interests pursued by the controllers
- an assessment of the necessity and proportionality of the processing operations according to their purpose
- an assessment of the risks to the data subjects, including safeguards, security measures and mechanisms to ensure the protection of personal data.

Impact assessment is a tool for timely identification, analysis and reduction of risks related to the misuse of personal data. Where it is possible that the nature of the processing, in particular using new technologies, given the nature, scale, circumstances and purposes of the processing, could lead to a high risk to the rights and freedoms of individuals, the controllers shall, prior to processing, evaluate the effect of the intended processing operations on the protection of personal data. Impact assessment can be applied and carried out for a single process of processing personal data or for several processes of (similar) processing of personal data.

In accordance with the GDPR, the following should be considered:

- that documented and enforced policies and support procedures for contacting the appropriate supervisory authority using an established consent mechanism to validate binding business rules in order to ensure that they are legally binding, include all necessary and appropriate data protection, are consistently enforced and comply with all legal requirements regarding the rights of individuals
- that the procedures to be followed for the transfer of personal data to a third country or to an international controller or processor are documented, stipulating that such transfer can only be carried out under certain and verified specified conditions (sufficiency, international agreement, verified existence of sufficient protection, enforceable rights of individuals and accessible and effective sanctions)
- that data security policies and support procedures and mechanisms for the protection of personal data during transmission are applicable in any case and are legally documented by public authorities, such as binding business rules, standard data protection provisions of the European Commission or the supervisory authority, codes practices or approved validation mechanisms.

5 Risk Assessment Methodology

There is no agreed definition of the notion of "risk" in the data privacy field. As stated, the GDPR also does not define the concept of "risk" and, instead, offers interpretative guidance on what may constitute risk and harm to individuals. The concept of "risk" appears to mean different things to different people, especially in a subjective domain like privacy, and is often used flexibly to apply to different components of "risk". For example, one might refer to the risk of a data breach, but the data breach itself does not necessarily lead to harm or damage for data subjects, depending on whether the data are ever looked at or manipulated. On the other hand, one might refer to the risk of losing confidentiality or financial loss, which are consequences that could result from a data breach. Similarly, "risk" is sometimes broadly used to refer to a risky processing activity or a "threat" that could result in damage for the individual, or damage to itself, or to both. That is also the approach that appears to be taken in Recital (75) of the GDPR, which seems to conflate the concepts of the risky processing activity and harm under the notion of "risk".

While there are numerous definitions and concepts of "risk" in the privacy and data security arena, the GDPR clearly focusses on one type of risk: adverse risk to the individual. Accordingly, we will focus in this paper on this aspect. Note that the assessment of the risks to individuals is closely related to other aspects of risk, especially as organisations incorporate their GDPR-based risk assessments that focus on adverse risks to individuals into their broader enterprise risk management systems that assess mainly risks to the organisation (such as reputational, financial and litigation risk) or corporate opportunity risks related to the organisation's business and profit objectives.

Because the GDPR distinguishes between different risk levels and associated obligations, it may invite the perception that the relevant assessment processes might be different for the different risk levels as well. However, the general risk assessment elements, factors and considerations, as well as the processes or methodologies for such risk assessments, must be the same for all instances in which risk assessment needs to be carried out and for all categories of risk (low, medium and high risk), as the actual level of risk can only be known at the end of the assessment process. Nevertheless, this does not suggest that a single risk assessment methodology needs to be selected and applied for all types of risks within the same organisation. The same methodology should be used for comparable processing operations in order to produce comparable results on the level of risk.

The GDPR provides minimal guidance on the risk assessment process, providing only that it must assess the likelihood and severity of risks, taking into account the nature, scope, context and purposes of the processing. It must also include an assessment of the necessity and proportionality of the processing in relation to its purpose, as well as an assessment of the risks to the rights and freedoms of the data subjects. In addition, it must include the relevant mitigation measures and safeguards, taking into account the rights and legitimate interests of the affected individuals.

5.1 The Basis for Identifying Potential Sources and Consequences of Risks

Privacy principles provide the basis for identifying potential sources and consequences of risks but are not sufficient to fully address and conduct a risk assessment.

Risk represents the effect of uncertainty on the goals set and the risk management of a concerted activity aimed at directing and controlling the organization in the area of risk.

Probability is the likelihood of an event.

Control is a measure that maintains or alters the risk and may include processes, policies, devices, processes and other conditions and / or activities that maintain and/or alter the risk.

When designing a risk management framework, an organization should consider and understand the external and internal contexts, so it is essential to understand and summarize at least the essential elements and nature of the processing of personal data in order to conduct a structured risk assessment.

The following processing activities qualify as potentially risky processing that may result in harm:

- processing of vulnerable persons' data, such as children's
- processing of large amounts of data affecting a large number of individuals
- engaging in a "new kind" of the processing
- automated processing, including profiling, that provides a basis for decisions with legal effect or similarly significant effect
- large-scale processing of special categories of data, and criminal conviction and offences data
- large-scale and systematic monitoring of publicly accessible areas
- use of new technologies.

A risk assessment should consider the potential threats in any given processing. Such threats include:

- unjustifiable or excessive collection of data
- use or storage of inaccurate or outdated data
- inappropriate use or misuse of data, including:
    - use of data beyond individuals' reasonable expectations
    - unusual use of data beyond societal norms, where any reasonable individual in this context would object
    - unjustifiable inference or decision-making, which the organisation cannot objectively defend
- lost or stolen data or destruction and alteration of data
- unjustifiable or unauthorised access, transfer, sharing or publishing of data.

Organisations must assess the likelihood and severity of any harms that might result from the risky processing or threats. Such harms may include:

- material, tangible, physical or economic harm to individuals, such as:
    - bodily harm
    - loss of liberty or freedom of movement
    - damage to earning power and financial loss
    - other significant damage to economic interests, for example, arising from identity theft
- non-material, intangible distress to individuals, such as:

- detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions
- the chilling effect on freedom of speech, association, etc.
- loss of reputational
- personal, family, workplace or social fear, embarrassment, apprehension or anxiety
- unacceptable intrusion into private life
- unlawful discrimination or stigmatisation
- loss of autonomy
- inappropriate curtailing of personal choice
- identity theft
- deprivation of control over personal data.

The process subtype defined by ISO 31000: 2018 [11] (shown in Figure 2) is used to perform the impact assessment analysis.

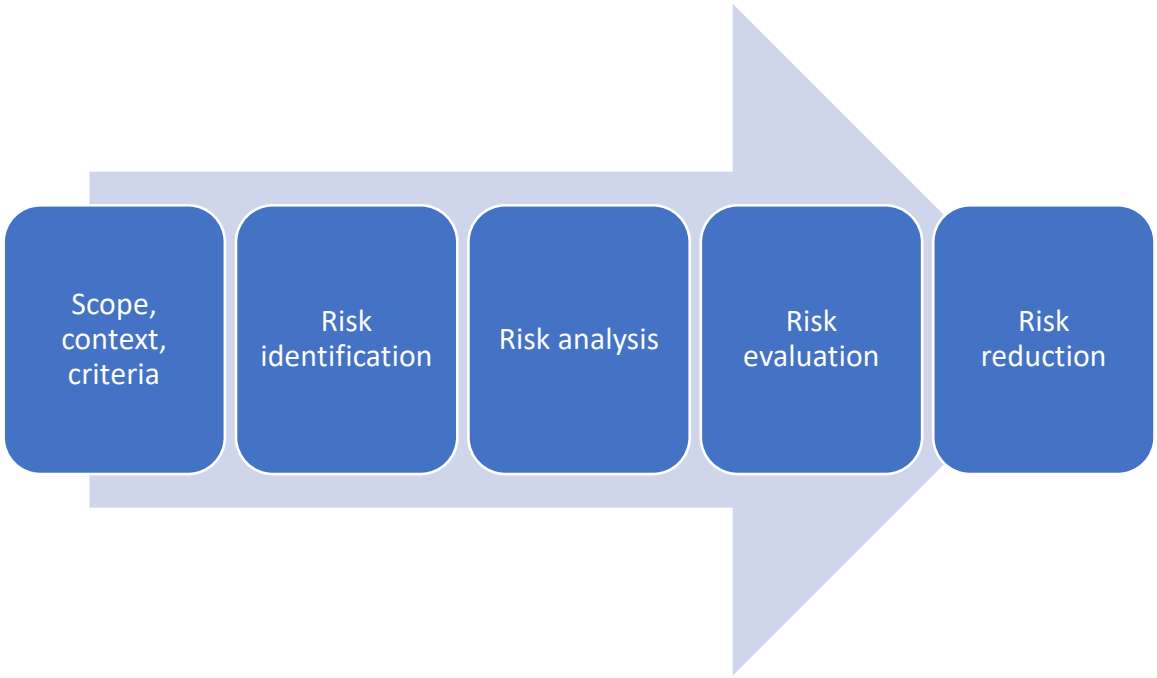

Figure 2: Activities within the risk management process for the purposes of analysing the impact on privacy

5.2 Risk Identification

Risk assessment is a process that integrates risk identification, risk analysis and risk evaluation.

In identifying risks, the ability to identify and describe risks that can affect the achievement of an organization's goals is essential. Therefore, up-to-date information is essential for identifying risks.

Risk identification is based on interviews and review of existing organization documentation in order to identify the essential actors, processes and data streams involved in the processing of personal data.

In order to identify the risk, the following should be considered:

- tangible and intangible sources of risk
- the nature and value of the resources
- traps and opportunities
- vulnerabilities and capabilities
- the consequences and their impact on the set goals
- the nature and value of the resources

The purpose of risk analysis is to understand the nature of the risks and their characteristics and where possible the level of risk.

According to the GDPR, risk analysis can be carried out with different levels of detail and complexity, depending on the purpose of the analysis, the availability and reliability of the information, and the resources available.

The analysis techniques can be qualitative, quantitative or combined, depending on the circumstances and purpose of the application.

As part of our methodology, we will use a combined analysis technique - qualitatively identifying individual risk factors and then addressing them quantitatively in order to objectify the risk assessment.

As part of the risk analysis technique, we have selected the following recommended GDPR factors:

- the likelihood of events and their consequences
- the nature and extent of the consequences
- the effectiveness of existing controls
- sensitivity and levels of confidentiality

The purpose of risk evaluation is to support decision making. The risk assessment, therefore, includes the results of the risk analysis against the established risk criteria in order to determine whether additional risk mitigation measures are needed. The following action decisions can be taken under the GDPR:

- no action
- consideration of risk reduction options
- carrying out further analysis to better understand the risks
- maintaining existing controls
- re-weighing goals

The purpose of risk reduction is to select and introduce risk reduction options. Risk reduction is a repeatable process that consists of:

- design and selection of risk mitigation options
- risk reduction planning and implementation
- assessing the effectiveness of risk reduction
- deciding whether the residual risk is acceptable

- where residual risk is not acceptable, further mitigate the risk

The privacy impact analysis focuses on the design and selection of risk mitigation options.

When choosing the options for risk reduction in accordance with the GDPR, we have taken into account the following:

- removal of the source of risk
- change in possibility
- change in consequences

Other options for risk reduction for the purposes of privacy impact analysis cannot be considered for various reasons:

- risk avoidance by discontinuing activities is not acceptable, assuming that the processes were optimally designed before performing the risk analysis (adequacy, proportionality and relevance analysis was carried out previously)
- accepting or increasing the risk of seizing the opportunity is unacceptable since it must take into account the impact on the rights and freedoms of the individual and not only the influence on the controller
- risk-sharing is not possible, as the controller is responsible for processing personal data and cannot share or transmit it (e.g. through insurance)
- informed risk acceptance is not an option, as this would be a conscious breach of personal data protection rules.

As part of risk mitigation, we will make recommendations for privacy risk mitigation; otherwise, privacy impact analysis is a process that is included into integrated risk management and does not interfere with other processes aimed at comprehensive risk management.

The preparation of a risk reduction plan and the implementation of the plan is beyond the scope and purpose of this privacy impact analysis.

As risk reduction is a recurring process, we will conduct a risk analysis against planned risk mitigation measures in order to provide information for deciding whether the remaining risk is acceptable.

5.3 Risk Criteria

The risk criteria are based on a quantitative assessment, supplemented by a word tag and a description of each level of possibility or severity for ease of understanding. In accordance with the ISO 31010 recommended ratios, we have selected a linear possibility/severity ratio.

Determining the risk level is essential for the following reasons:

- to deliver effective and high-level privacy and data protection for individuals
- to gather information on specific mitigations and controls that accountable organisations are required to implement to ensure GDPR compliance

- to determine whether there is “high risk” that would trigger specific compliance obligations under the GDPR, such as the obligation to undertake a data protection impact assessment, or to notify individuals of a data breach.

For the purpose of establishing quantitative risk criteria, the following possibility levels for an individual event are determined:

- 0 - Not possible because we do not carry out this type of processing of personal data or this type of activity.
- 1 - **Low** when the likelihood of an event is less than once a year, rapid elimination of consequences (same day), proven compliance with regulations.
- 2 - **Medium** in the event that the probability of an event of up to two times a year is acceptable elimination of consequences (not later than the next day), it is not reliable, or all the requirements of the regulations are met.
- 3 - **High** when the probability of an event is up to once in half a year, acceptable elimination of consequences (not later than the next day), the requirements are not reliably fulfilled.

For the purpose of quantitative risk criteria, risk or severity levels are determined for the purpose of assessing individual risk:

- 1 - **Low** when the consequences of an event will have no effect on the rights and freedoms of the individual or the consequences for the rights and freedoms of the individual will be negligible.
- 2 - **Medium**, when the consequences of an event could have an effect on the rights and freedoms of the individual, which can be mitigated in an acceptable time and with reasonable effort.
- 3 - **High** when the consequences of the event will have a significant impact on the rights and freedoms of the individual, which cannot be mitigated or can only be mitigated after a long time and with great effort.

On the basis of quantitative criteria, we have developed a risk matrix, by means of which we have determined the levels of threat that represent a low, medium or high level of threat to the rights and freedoms of an individual with regard to the processing of personal data.

The threat matrix (Table 5) follows the recommendations in Annex B.29 for the consequence/probability matrix according to the ISO 31010 [11].

		Probability	
Severity	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

Table 5: Threat matrix

Regardless of the semi-quantitative approach chosen, in which the final threat is expressed numerically and converted to a qualitative description, according to the ISO 31010 it should be borne in mind that the

result of the risk analysis is still only an estimate and does not represent an objective quantified by any of the recommended techniques.

The effectiveness of controls is assessed on the basis of documentation of business processes and interviews, and is not based on a detailed examination of the effectiveness of the operation of individual controls, but rather the assessment relies on the functioning of controls, insofar as information exists that controls exist.

The next table (Table 6) presents a matrix that can be used for assessing the relevance and proportionality of personal data. The table after that (Table 7) is a legend of compliance levels.

N.	DATA TYPE	REQUIRED DATA (YES/NO)	DATA RETENTION PERIOD	LEGAL BASIS	NOTES	COMPLIANCE
1						
2						

Table 6: Matrix for assessing the relevance and proportionality of personal data

Level	Description of compliance level	Measures
1	The information is unlikely to be relevant or its processing probably does not represent proportionate processing of personal data. In cases where the information is not specified in the regulations, when the purpose or type of processing may be questionable in relation to the regulations and where the information is probably not necessary to achieve the purpose of the processing.	Finding alternative data processing solutions. Interruption of data collection and processing.
2	The information is probably relevant, and its processing is likely to constitute proportionate processing of personal data according to the purpose of the processing. In cases where the processing of personal data is indirectly or unclearly determined by law, in the case of open definitions of the content of the data in the regulations and in cases where the data is not essential in all respects to achieve the purpose of the processing (e.g. the purpose of processing can be achieved but with more effort).	Particular care in examining and validating the analysis. Relevance and proportionality should be analysed by several experts, if necessary in the form of a workshop. When reviewing an analysis, a DPO review is required when appointed.
3	The information is no doubt proportionate and relevant to the processing of personal data. In cases where the processing of personal data is explicitly and unambiguously determined by the regulations and where it is indisputable (it is obvious) that the essential goals of the processing cannot be achieved without this data.	No additional action is needed.

Table 7: Legend of compliance rates

5.3.1 Assessment of Relevance and Proportionality of Personal Data Processing

Please analyse and explain whether you are collecting and processing only the data relevant to achieve the goal of processing. Check the legal basis for the processing of all identified data types.

5.3.2 Assessment of the Risks to Individuals' Rights and Freedoms

According to implemented controls, complete the table (Table 8) with the probability and severity of identified risks and calculate the final risk value. Use threat matrix to calculate the risk value.

Identified threats are baseline only. Feel free to add and modify baseline threats.

For probability and severity use levels as defined in the threat matrix (i.e. low, medium, and high). For every risk, group use the highest identified risk as risk level for the whole risk group.

	RISK	PROBABILITY	SEVERITY	RISK
CUMULATIVE VALUE				
1 Choice and consent				
1	There is no legal basis for processing			
2	The legal basis is not properly selected			
3	Use of legitimate interest by public authorities in the performance of their tasks			
4	The conditions for consent are not clear			
5	The terms of consent are not separated by purpose			
6	An individual is unlawfully coerced into consent in an incompatible relationship with another lawful ground			
7	Consent is not clearly different from other matters			
8	Consent is not in clear and simple language			
9	The consent may not be revoked at any time by an individual			
10	Consent is not as easy to revoke as to give			
11	Risks related to the processing of children's personal data			
2 Determination of lawful purpose and limitation of use				
12	The purpose of the processing is not specified			
13	The purpose of the processing is not explicit or clearly defined			
14	The purpose of the processing is not legal			
15	The retention period is not set			
16	Use of data for another purpose than the purpose for which it was collected			
17	Excessive data volume for processing (minimum data volume not used)			
18	Retention period exceeded			
19	The processing method does not guarantee the security			

	of personal data
20	There is no protection against tampering or illegal processing
21	There is no protection against unintentional loss or destruction of personal data
22	There is no protection against accidental data corruption
23	Risks related to automated decision making
24	Risks related to profiling
3 The life cycle of personal and sensitive information	
25	Extension of retention period with no legal basis
26	Failure to extend the retention period, where there is a legal basis or at the request of the individual
27	Undefined procedures of the individual's request after verification if the controller processes data
28	Undefined procedures of the individual's request for access to data processed by the controller
29	Undefined procedures for individual’s requests after restriction of processing
30	Undefined procedures for individual’s requests after data deletion
31	Undefined procedures of the individual's request for data portability
32	Undefined procedures in case of an individual's objection
33	Improper implementation of procedures in case of an individual’s request to verify that the controller is processing data
34	Improper implementation of procedures in case of individual’s request access data processed by the controller
35	Improper implementation of procedures in case of individual’s request
36	Improper implementation of procedures in case of an individual’s request for deletion of data
37	Improper implementation of procedures in case of an individual’s request for data portability
38	Improper implementation of procedures in case of the objection of an individual

39	Unnecessary processing of specific types of personal data
40	The implementation of information systems and the design of processes do not take into account data protection by default and by design
41	No data protection impact assessment has been produced
4 Punctuality and quality	
42	The information is incorrect
43	An individual's data is not updated when the individual changes it
44	In the case of data change, not all data of the individual is updated
45	Undefined procedures in case of an individual’s request for rectification of data processed by the controller
46	Improper implementation of procedures when requesting an individual to correct data processed by the controller
5 Openness, transparency and informing	
47	The information is not transparent to the individual
48	Information presented to the individual is not uniform for all controllers and processors
49	Ways to exercise the rights of the individual are not given in a comprehensive and clear manner
50	Information is not provided to an individual when obtaining personal information
51	Inaccurate informing of an individual when information is not obtained from an individual
6 Participation of individuals	
52	The portable data received by an individual are not machine-readable
53	The portable data received by an individual is incomplete
54	The decision made by automatic decision-making is final
55	Automatic listing of an individual is definitive
56	For the joint controllers, the agreement does not clearly set out all the rights and obligations of each of the controllers

57	The content of the joint controller's agreement is not accessible to the individual
58	There is no designated contact point for the individual
59	The contract unlawfully restricts the exercise of individual rights to certain controllers
60	There is no designated data protection authority
61	The contact details of the Data Protection Officer are not accessible to the individual
7 Responsibility	
62	There is no defined procedure for determining whether the processing of personal data for other purposes is legal
63	The tasks and responsibilities of the Data Protection Officer are not clearly defined
64	There is no defined procedure for consulting the supervisory authority in light of the results of the privacy impact analysis
8 Security measures	
65	There are no documented security policies for protecting personal information
66	There is no documented processing of personal data for purposes other than the purpose for which they were collected
67	Organizational measures for the protection of personal data are not clearly defined
68	There are no clearly defined technical measures for the protection of personal data
69	Organizational measures to protect personal data are not sufficient
70	Technical measures to protect personal data are not sufficient
71	Organizational measures to protect personal data are not being implemented
72	No technical measures are in place to protect personal data
73	There is no regular check on security controls
74	Organizational controls for the protection of personal data are not clearly defined in contracts with processors
75	Technical control contracts for the protection of

	personal data are not clearly defined in contracts with processors
9 Monitoring, measuring and reporting	
76	The Data Protection Officer does not guarantee the implementation of privacy impact assessments
77	The Data Protection Officer does not check compliance with the regulations
78	The Data Protection Officer does not educate employees
79	The Data Protection Officer does not cooperate with the supervisory authority
80	No reporting regarding the correction of personal data is introduced
81	No reporting regarding the deletion of personal data is introduced
82	There is no documented content reporting on an individual's personal information
83	Reporting on the transfer of individual data to third parties is not introduced
84	Copies of personal data provided as part of the right to data portability have been preserved longer than the retention period
85	No triggers have been identified to produce a privacy impact analysis
86	There are no policies in place to design and maintain records of processing activities
87	Recipients of personal data are not identified
10 Prevention of damage	
88	Guidelines for determining the legality of processing have not been established
89	No consequences are determined for the individual in case of further processing of personal data
90	There is no adequate safeguard for decision making based on specific types of personal data
91	There is no guarantee that the exercise of an individual's right will not adversely affect the rights and freedoms of others
92	No rules and procedures have been put in place to minimize the harm to an individual when archiving in

	the public interest
93	No rules and procedures have been put in place to minimize harm to an individual for use of their personal data in historical and scientific research purposes
94	No rules and procedures have been put in place to reduce harm to an individual for statistical use of their personal data
11 Supplier / third party management	
95	No outsourcing management policies are in place
96	Outsourcing arrangements do not contain sufficient guarantees that adequate organizational measures are in place to protect personal data
97	Outsourcing arrangements contain sufficient guarantees that adequate technical measures are in place to protect personal data
98	Sufficient restrictions and rules for hiring sub-contractors have not been applied
99	Procedures and duration of processing are not specified in the agreement with the processors
100	The purpose and type of processing is not specified in the agreement with the processors
101	The types of personal data subject to processing are not specified in the agreement with the processors
102	The types of individuals whose personal data are subject to processing are not specified in the agreement with the processors
103	In agreement with the processor, not all 8 obligations are specified as per Article 28 paragraph 3 of the GDPR
104	The agreement with the processor does not specify the obligation and the procedure for reporting incidents
105	There are no requirements for the processor to outsource his work
106	There are no procedures in place to ensure that processors comply with the requirements of the controller
107	There are no procedures in place for the employee of the controller to comply with the requirements of the controller

12 Management of incidents	
108	Procedures for notifying the supervisory authority of incidents have not been established
109	Procedures for notifying individuals of violations are not specified
110	The content of the notice is not specified in accordance with the regulations
13 Built-in security and privacy	
111	Privacy and security policies do not respect the rights of the individuals
112	Privacy and security policies do not respect the freedoms of the individuals
113	Privacy and security policies do not take into account the legitimate interests of the individuals
114	Automatic procedures do not involve human intervention
115	No policies have been put in place to assess the nature, extent, context and purposes of the processing of personal data
116	An impact assessment on an individual is not an input to the requirements for designing information solutions
117	Harm reduction for an individual is not an integral part of the process of creating information solutions
14 Free movement of information and legal restriction	
118	No procedures for validating binding business rules have been defined
119	No data transfer procedures are defined at the request of other persons
120	Data transfer procedures to a third country are not defined
121	No data protection procedures are in place for their transmission

Table 8: Risk assessment

5.3.3 Analysis of the Risk Assessment of Individuals' Rights and Freedoms

Transfer the highest identified risk levels from the “Risk assessment” table to the following matrix (Table 9) to identify the highest risk.

Risk group	The highest risk
1 Choice and consent	
2 Determination of lawful purpose and limitation of use	
3 The life cycle of personal and sensitive information	
4 Punctuality and quality	
5 Openness, transparency and information	
6 Participation of individuals	
7 Responsibility	
8 Security measures	
9 Monitoring, measuring and reporting	
10 Prevention of damage	
11 Supplier / third party management	
12 Management of incidents	
13 Built-in security and privacy	
14 Free movement of information and legal restriction	

Table 9: Risk group overview by risk group

6 The Opinion of the Data Protection Officer

Based on Article 35 paragraph 2 of the GDPR after the implementation of a data protection impact assessment, the Controller shall request the opinion of the Data Protection Officer, where it is appointed, for an opinion.

The controller can ask the Data Protection Officer for the opinion on:

- whether or not to carry out a data protection impact assessment
- what methodology to use when conducting the data protection impact assessment
- whether to carry out the data protection impact assessment internally or outsource it
- what safeguards (including technical and organizational measures) to use to reduce potential risks to the data subjects' rights and interests
- whether the data protection impact assessment was properly carried out and whether its findings (whether processing should continue or not and what safeguards should be applied) are in accordance with the GDPR.

Data Protection Officer after formally adopting a data protection impact assessment in accordance with point Article 39, Paragraph 1(c) of the GDPR assumes the task of overseeing the implementation of the data protection impact assessment.

When the impact assessment is done, the controller should also take care that the impact assessment is updated at regular intervals, meaning any major change in regulations, business processes, data, purposes or type of processing of personal data. If changes from the environment have not triggered a refreshment within three years, it is obligatory to refresh the impact assessment within three years at the latest.

Insert here any additional comments or responsibilities of the DPO regarding DPIA analysis.

7 Self – assessment

With a view to self-assessment of the conformity of prepared DPIA with the regulations, self-assessment of the produced impact assessment is carried out according to the DPIA adequacy assessment criteria in accordance with the guidelines on the Data Protection Working Party's data protection workgroup (Table 10) referred to in article 29 16/SL WP 243 Rev. 01.

Requires	Reference	Self-assessment
A systematic description of the processing is provided (Article 35 (7a))		
The nature, extent, circumstances and purposes of the processing are taken into account (Recital 90)		
The data set, controllers and users, and retention periods are defined		
A description of the data flows and the entities involved is given		
Description of processing assets (hardware and software, networks, human resources and the means of communication used)		
Compliance with approved codes of conduct (Article 35 (8))		
Necessity and proportionality are assessed (Article 35 (7b)) and measures are laid down to ensure consistency, which includes measures contributing to compliance with necessity and proportionality and respect for fundamental principles		
Specific, explicit and legitimate purposes (Article 5 (1b))		
The legality of processing (Article 6)		
The processing is relevant and limited to what is necessary for the purposes, for which the data are processed (Article 5 (1c))		
Storage limit respected - Retention periods are respected (Article 5 (1e))		
Necessity and proportionality are assessed (Article 35 (7b)) and compliance measures are defined which include measures that contribute to the protection of the rights of the individual		
Informing an individual of data processing (Articles 12, 13 and 14)		
Right to be informed and to portability (Articles 15 and 20)		
Right to rectification and to be forgotten (Articles 16, 17 and 19)		
Right of objection and restriction on processing		

(Articles 18, 19 and 21)		
Relations with (contract) processors (Article 28)		
Controls when transferring data to third countries (Chapter V.)		
Prior consultation (Article 36)		
The risks to the rights and freedoms of the individual are managed by assessing the origin, nature, specificity and severity of the risks (recital 84), whereby the risks are assessed from the perspective of the individual so that		
Sources of risk to be taken into account (Recital 90)		
The potential effects on the rights of the individual in the case of unlawful access, changes or loss of data are considered		
The likelihood and severity of the risks are assessed (Recital 90)		
The risks to the rights and freedoms of the individual are managed		
Risk management measures are defined (Article 35 (7d) and Recital 90)		
Stakeholders are included		
The opinion of the DPO (Article 35 (2))		
Opinions of individuals or representatives of individuals, where applicable and appropriate, are obtained (Article 35 (9))		

Table 10: Self – assessment

8 Member States Special Requirements

GDPR allows Member States some freedom regarding detailed privacy regulation. Therefore, any data processing operations that are expected to cross Member State borders should take that into account.

This document is not intended to cover special requirements for all Member States. Just for illustration, we are providing a map of some of Member States (and some European Economic Area) regarding the use of biometrics for access control in the private sector (red – not allowed, orange – allowed under special requirements, green - allowed). The list is limited to the states that have answered an online survey that was sent to the project partners.

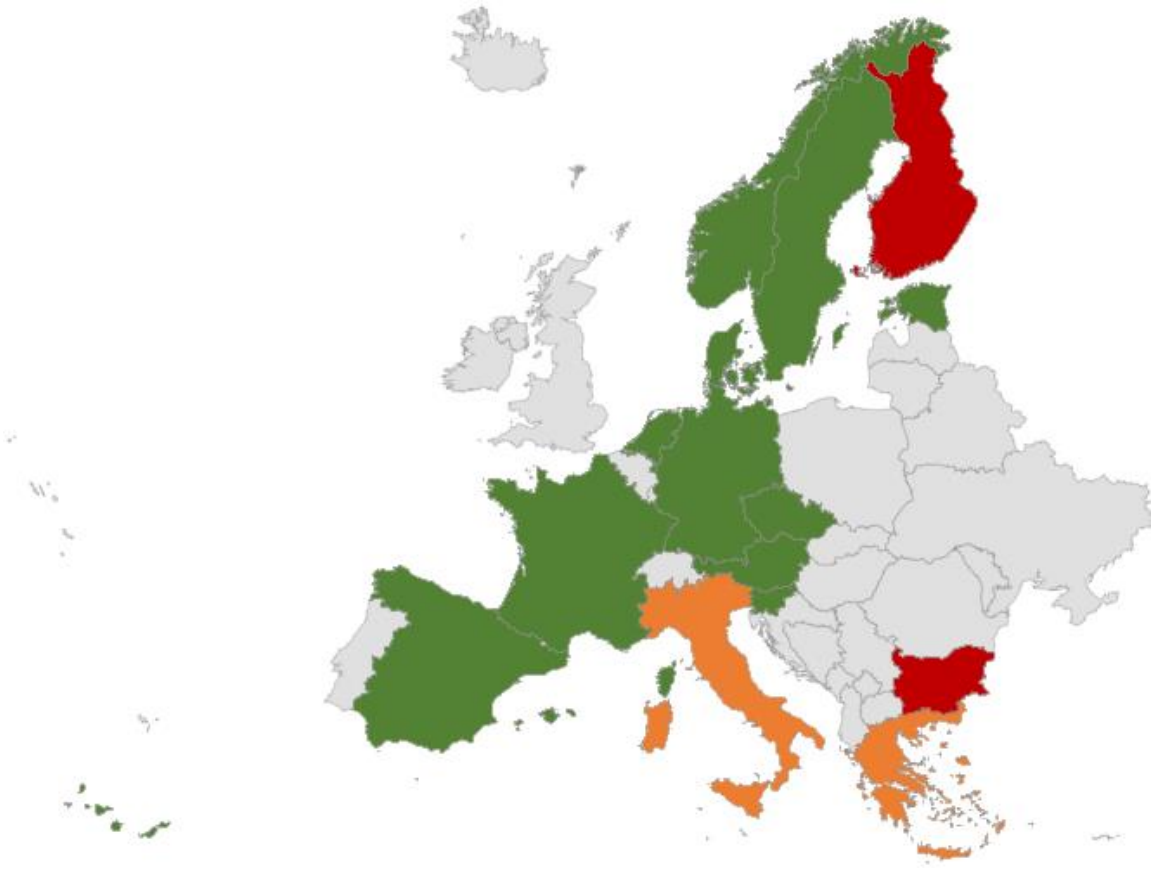

Figure 3: Use of biometrics for access control in some Member States

Further, some Member States have decided to regulate minimum consent age (green – 16 years (same as in GDPR), blue – 15 years, orange – 14 years, red – 13 years).

There may be other regulated areas requiring special attention if data processing relates to individuals in those Member States. This document is not a complete tool to address such cases.

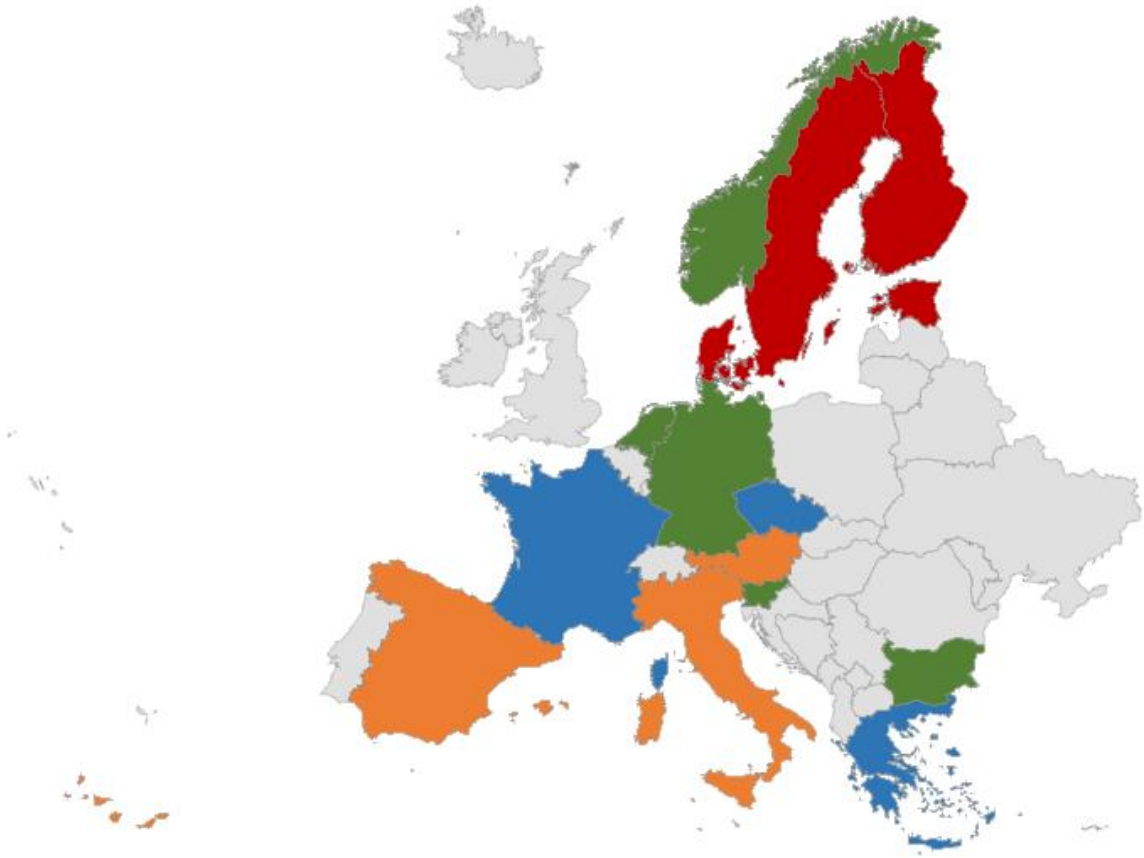

Figure 4: Minimum age for consent under the GDPR

9 Conclusion

GDPR privacy requirements for controllers and processors are quite extensive and require a lot of effort to implement properly.

Even when controllers and processors follow the designed methodology and with strict care for compliance, the issues with cross-border compliance within the EU will remain. GDPR allows Member States some freedom regarding privacy governance. For cross-border service providers, these issues will manifest in additional effort required for full GDPR compliance in all Member States. This will have an impact on the overall efficiency of service providers in the Single European Market and can also affect cross-border competitiveness in some Member States.

For example, not all Member States allow the use of biometrics to acquire hand-written signatures. Some even prohibit or limit the use of biometrics for access control in the private sector. The consequence of the first is an additional burden for service providers with a paper signed documents, their management and archiving. The consequence of both is limited compliance of services or products developed for one Member state in the other Member States.

Similarly, differences in the minimum age for consent will require service providers to adapt to differences in the Member States in their software and other solutions. Though implementing this may seem trivial, it is not so straightforward to understand, collect and follow different requirements in all Member States. We should also consider that some local regulations are not translated (to any of the other official EU languages).

We have considered implementing a service to check minimum consent age for Member States. The main issue with such a service is in promptness to changes in regulation in all Member States. Considering the structure of partners in this project and the intent of the network, we found that it would not be trivial to implement an alerting service to regulatory changes in the existing partner network. Therefore, further research in organizational options to follow such changes is needed to understand the possibilities and impacts of such a technical service on the final compliance and responsibilities for involved subjects.

10 References

[1] APEC Privacy Framework, (2015). https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).

[2] Canadian Institute of Chartered Accountants (CICA) and American Institute of Certified Public Accountants, Generally Accepted Privacy Principles, (2009).

[3] ISACA, GDPR Data Protection Impact Assessments, (2017). http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/GDPR-Data-Protection-Impact-Assessments.aspx.

[4] ISO/IEC 29100:2011 Information technology — Security techniques — Privacy framework, https://www.iso.org/standard/45123.html.

[5] Article 29 Data Potection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, (2017). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[7] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. https://a-lign.com/iso-27701-gdpr/.

[8] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. https://www.iso.org/standard/54534.html.

[9] ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. https://www.iso.org/standard/54533.html.

[10] Article 29 Data Potection Working Party, Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector, 2016. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640147.

[11] ISO 31000:2018, Risk management — Guidelines. https://www.iso.org/standard/65694.html.