Risk Assessment & Data Protection Impact Assessment

Guide

bitkom

Publisher

Bitkom e. V.
Federal Association for Information Technology, Telecommunications and New Media
Albrechtstraße 10 | 10117 Berlin

Contact

Susanne Dehmel | Member of Executive Board for Law & Security
T 030 27576-223 | s.dehmel@bitkom.org

Responsible Bitkom Working Group

WG Data Protection

Graphics & Layout

Per Dittmann | www.perdittmann.net

Cover

© zazamaza – iStock.com

Risk Assessment & Data Protection Impact Assessment

Guide

Table of Contents

Preface

The General Data Protection Regulation will, from 25 May 2018 onward, implement new legal obligations to ensure data security in data processing. The overarching principle is that of accountability. Companies must not only implement data protection compliant data processing processes, but must also be able to document their compliance. For certain areas, these obligations are described in detail in the GDPR. For example, Article 32 of the GDPR implements a risk-based approach for the implementation of technical and organizational measures to achieve security in processing. Therefore, companies will have to carry out comprehensive risk assessments, and the evaluations of IT security and data protection will continue to converge. The data protection impact assessment, as defined in Article 35 of the GDPR, also entails the obligation to document the comprehensive risk assessments and the planned remedial measures in a manner appropriate to the requirements of the law. A data protection impact assessment is also required for particularly risk-sensitive data processing.

This guide provides a detailed description of how companies can meet the requirements of the GDPR and can adapt their risk management to the GDPR. The guide is an important tool in the implementation of the new requirements, with detailed instructions to ensure security in the processing and the preparation of a data protection impact assessment

We should like to specifically thank the following members of the Data Protection Working Group for their expertise and valuable practical experience, which have made a major contribution to the development of this guide:

- Rudolf Bertold Gerhard, DATEV eG
- Sebastian Brüggemann, IBM Deutschland GmbH
- Rudi Kramer, DATEV eG
- Heiko Gossen, migosens GmbH
- Ilona Lindemann, gkv informatik GmbH
- Stephan Rehfeld, DQS GmbH und scope & focus Service-Gesellschaft mbH
- Anna Täschner, ePrivacy GmbH
- Vito Tornambé, Deutsche Post
- Marion Weimer-Hablitzel, Deutsche Post AG

The charts and diagrams were developed by Mr. Rehfeld (S.), Mr. Gossen (S.), and Mr. Gerhard (S.).

The Data Protection Working Group consists of experts of Bitkom Members and deals with current topics and data protection-specific aspects of the information and communication technology. A profile of the Working Group can be found at the end of this guide.

1 Introduction

1 Introduction

Any data processing within the company must be compliant with data protection requirements and any company must be able to demonstrate this conformity in accordance with the accountability obligations. The topic of risk assessment/data protection impact assessment ("DPIA"), which is dealt with in this guide, is a component of the overall concept of the GDPR for data protection-compliant data processing.

For German data protection officers, § 9 of the Federal Data Protection Act (BDSG) with Annex 1 to § 9 sentence 1 BDSG was the basis for the assessment of the technical and organizational measures. Additionally, § 4(d) of the BDSG stipulated that a prior checking should be carried out under certain conditions. Both obligations are reflected in changed form and under modified terms in the GDPR. Article 32 of the GDPR now specifies the "security of processing" and, in Article 35 of the GDPR, the data protection impact assessment. Both articles describe the responsibilities of the controller, whereby Article 32 of the GDPR also applies to processors.

Compared to the current legal situation under the BDSG, the system for evaluating technical and organizational measures is changing. According to Article 32 of the GDPR, the assessment is based on the likelihood of occurrence and the severity of the risk for the rights and freedoms of natural persons. In many companies, the measures to be implemented have already been assessed with regard to risk related aspects - often in accordance with an information security management system ("ISMS"). However, there were also uncertainties as to whether the legal requirements were always met, since § 9 BDSG spoke of necessity, appropriateness and suitability. With regard to Article 32 of the GDPR, the methodology now used is one which is already known to many from the classical risk analysis and risk assessment.

Similar to the current legal situation, all procedures and systems that process personal data must be subjected to a risk analysis. As already established in many companies, a distinction can be drawn between "standard security", which basically applies to all procedures, and procedure-specific measures. Thus, the documentation effort per procedure is reduced to the determination and description of the delta to the overall security concept.

The data protection impact assessment (Article 35 of the GDPR) is the counterpart to the previously known prior checking (Article 20 of Directive 95/46/EC as e.g. implemented in § 4(d) of the BDSG). In contrast to the Directive, the company's data protection officer is now no longer obliged to perform the prior checking, but rather the controller himself. Until now, the exceptions to the requirement of a prior checking were stipulated in the national data protection laws such as the German BDSG. Under the new Regulation, the supervisory authorities will enumerate situations in which the data protection impact assessment is mandatory and when it is not required. There will probably be a large number of procedures which do not appear on any of the lists and which, according to the requirements of Article 35(1) of the GDPR, must be assessed with regard to the necessity of a data protection impact assessment. However, similar to the current situation, it is to be assumed that the data protection impact assessment does not have to be carried out for every individual procedure, but rather be the exception.

Therefore, appropriate processes within the company should ensure that a risk assessment is carried out for all procedures and, depending on the result

- Additional measures are planned and implemented in accordance with Article 32 of the GDPR and /or
- A data protection impact assessment is conducted.

It should be noted that the evaluation of the security of the processing is a subset of the data protection impact assessment:

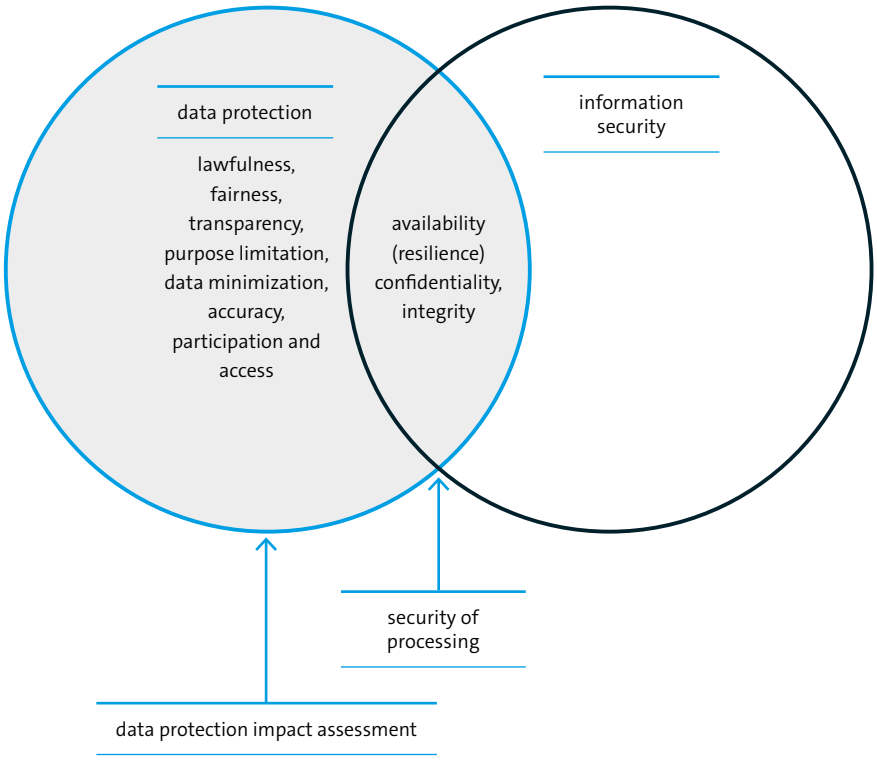


fig. 1: Overlap Data Protection and Information Security

Article 32 and 35 of the GDPR are built on each other, which is also reflected in the conception of this guide. The evaluation of the security of processing must generally be carried out when processing personal data. The results, in turn, are part of a possible data protection impact assessment.

The following chapters describe the standard requirements and give suggestions for how these can be implemented. It should be noted that, depending on the company's situation and the subject of the processing, more or less detailed considerations of the risks may be necessary. Also, the specifics of the implementation of the processes may vary widely.

2 Risk-based Approach

2 Risk-based Approach

Risk in the GDPR

Although the European legislator repeatedly refers to the concept of risks for the rights and freedoms of the data subjects, the term risk is not defined in the GDPR. Recital 75 only describes the adverse effects of the infringement of the rights of natural persons: "The risks to the rights and freedoms of natural persons, of varying likelihood and severity [...] which could lead to physical, material or non-material damage [...] or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms [...]."

In April 2017, the Article 29 Working Group published guidelines on data protection impact assessment and on the determination regarding the question whether a processing under Regulation 2016/679 is likely to be a "high risk" (Working Paper 248)[1] . The paper also deals with the question as to when a data protection impact assessment should be carried out and what the components of such an assessment should be. However, the guideline also does not define the term "risk".

Data Protection Risks in an International Context

In Europe and internationally, the supervisory authorities and the ISO have been dealing with data protection risk management as well as the data protection impact assessment (or: Privacy Impact Assessment, PIA) for several years and have developed and published proposals for implementation, which are also reflected in the Guidelines of the Article 29 Working Group:

Europe

- Great Britain - ICO. (2014)
  ↗ https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- France – CNIL (2015) ↗ https://www.cnil.fr/fr/node/15798
- Spain – EIPD, (AGPD) (2014) ↗ https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- Germany – Standard Datenschutzmodell, V 1.0 – Trial Version (2016)
  ↗ https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf

1 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 ↗ **http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083**

North America

- Canada – OPC ↗ https://www.priv.gc.ca/information/pia-efvp/index_e.asp

New Zealand

- OPC ↗ https://www.privacy.or

ISO

- ISO/IEC FDIS 29134 – Information technology -- Security techniques -- Guidelines for privacy impact assessment

The ISO also provides a catalogue of definitions for risk assessments:

ISO/Guide 73:2009(en) Risk management — Vocabulary -
↗ https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

In line with EU-wide standardized data protection, this guide will also be based on the existing work of European supervisory authorities, and will explain the operational practice with regard to the requirements of the GDPR. Furthermore, connections to other standards will be made at various points, above all to ISO / IEC 27005: 2011 for risk management. This is to support an integrated approach between data protection and information security. Users are hereby made aware of the work of the French supervisory authority (CNIL), which has done extensive preparatory work especially in the field of risk methodology. The example in this guide is also based on the CNIL methodology.

Users in an internationally set up company should consider the implementation of a Privacy Impact assessment with the ISO/IEC FDIS 29134:2017[2] standard. ISO / IEC FDIS 29134: 2017 provides a business model for a complete data protection impact assessment. The approach of ISO / IEC FDIS 29134: 2017 is compatible with the work of CNIL.

The abovementioned standards of the French supervisory authority and the International Organization for Standardization (ISO) do neither address the integration of the data protection impact assessment into the existing management systems nor a separate data protection risk management system. Again, we refer to international best practices. The risk management framework of ISO 31000: 2011 provides practical support.

2 Currently this standard is available as FDIS and is just before being adopted on international stage.

3 Prerequisite for Implementing Articles 32 and 35 GDPR: the Processing Records

3 Prerequisite for Implementing Articles 32 and 35 GDPR: the Processing Records

Although processing records according to the GDPR must only be maintained in companies with at least 250 employees, it is indispensable for data protection management. It is the authors' opinion that companies should be allocated into groups based on defined processing activities or procedures, as this is useful in order to divide the obligations of the GDPR into workable portions and to document these in a comprehensible manner.

This guideline is based to a large extent on the fact that there is already a processing record in place, or a "processing directory", or at least a structure or grouping of processing activities based on the different processes, business transactions, or processing activities. How such a structuring can be developed is described in the guide "↗ the Processing Records", which is referred to at this point.

> A processing record is the basis for implementation of the requirements in Articles 32, 35, and 36 of the GDPR. Without this tool, almost every data protection risk assessment will fail due to operational complexity.

The possible implementation of Articles 32, 35, and 36 of the GDPR will be illustrated by means of the business procedure of invoicing. For this purpose it is advisable to describe the method:

Example, general procedure

type of processing	Invoicing
purpose of processing of personal data	Preparation of offers and invoices, interface to financial accounting
interested parties	prospective buyers, customers, controller
controller	Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt

It should be noted that the column “interested parties” complements the abovementioned information on the procedure. Data Protection is essentially the protection of fundamental rights. An assessment of the data protection related consequences can therefore only be conducted from the data subject’s perspective. Irrespective of this point of view, however, it is also advisable to consider the point of view of other interested parties or, if these have already been considered in the risk management process, merge the different views. As a result, synergies can often be created.

Example of the documentation of data subjects, data, or data categories and retention periods*

data subject	creditor, deptor	employee
categories of personal data	name, company, address data, invoice data, bank account information	protocol data
personal data		user-ID, activity/ action, date, time
recipient of personal data	in-house: consultant, management, supervisors	in-house: management, head of accounting
access to personal data	suppliers: service technician, person erasing the storage mediums	suppliers: service technician, person erasing the storage mediums
retention period	offers, rejected: immediately; offers, accepted: 6 years; invoices: 10 years; tax relevant emails: 10 years	protocols: erasure after task fulfillment, 3 days

Note

* This is only part of the overall processing documentation, which is described in more detail in Bitkom's Guide ´the Processing Records´.

4 Security of Processing (Article 32 of the GDPR)

4 Security of Processing (Article 32 of the GDPR)

When processing personal data, the controller and the processor must provide an appropriate level of protection for the personal data of natural persons and demonstrate the effectiveness of the measures taken. The following part describes how the appropriate level of protection can be identified and how it can be implemented and maintained within the framework of a management system.

4.1 Appropriate Security Measures

Article 32 of the GDPR defines the requirements for the security of the processing. In contrast to the legal landscape up to May 2018, the system for determining suitable technical and organizational measures is now explicitly based on an assessment of the identified risks. An assessment and the adoption of measures based on the risks is not new to companies, for example, many of them already have a risk management system in place for information security risks. However, the approach taken in the GDPR differs somewhat from the considerations solely from the perspective of information security.

Article 32(1) of the GDPR requires the controller and the processor to ensure that appropriate safeguards are taken to protect personal data:

> "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

The risk orientation in the selection of information security measures is not new; at least in the BDSG, it was described in § 9 sentence 2 as proportionality of the technical organizational measures.

> "Measures shall be required only if the effort involved is proportionate in relation to the desired level of protection."

The very clear description of the method to be used (risk orientation) suggests a comparison with international standards for management systems. In data protection and information security, we use the same principles to assess the security of personal data and the security of information, but evaluate it from different perspectives:

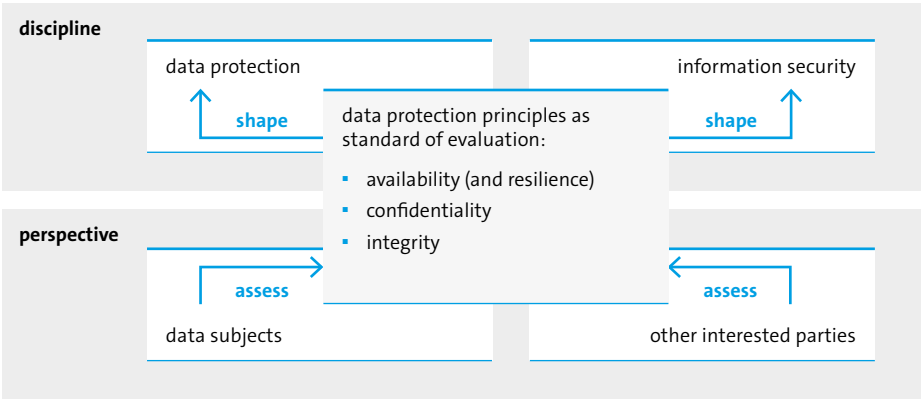


fig. 2: perspective of information security and data protection

Because of the different perspectives, the results obtained from information security cannot simply be adopted for data protection, provided that the risks for the freedoms and rights of the data subjects have not already been sufficiently taken into account in the existing methodology. The results of data protection and information security risk assessment may coincide, but not necessarily.

Example: Applicant Database

A company uses an online application platform where applicants can register and update their application data. However, the authentication method is weak because the user name corresponds to the applicant's email address and there are no requirements with regard to length and complexity of the password.

A mere view of the potential loss for the company would determine a low risk with regard to the loss of confidentiality (e.g. by a hacked applicant account), since the company would not suffer direct damage. With regard to the obligation under Article 32 of the GDPR, however, the potential damage for the data subject will also have to be taken into account, for example, his own economic damage, as the fact of his application including all application documents is now publicly known. This can thus lead to a changed result of the risk assessment and thus also necessitate further measures of risk management.

4.2 Implementation of the Protection Level with the Help of a Management System

In Article 32(1)(d) of the GDPR the European legislator describes the requirements for monitoring the technical and organizational measures, which has been practiced for (information security) management systems (ISMS) for years already: “a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing”.

This rather inconspicuous sentence now obliges companies not only to carry out appropriate processes but also on a regular basis. But here, too, sensible synergies with information security management can be built.

1. The PDCA cycle is used as the motor of the management system.
2. The phases of risk assessment, the preparation and implementation of a risk management plan, internal audits, management assessment and taking corrective actions are stipulated..

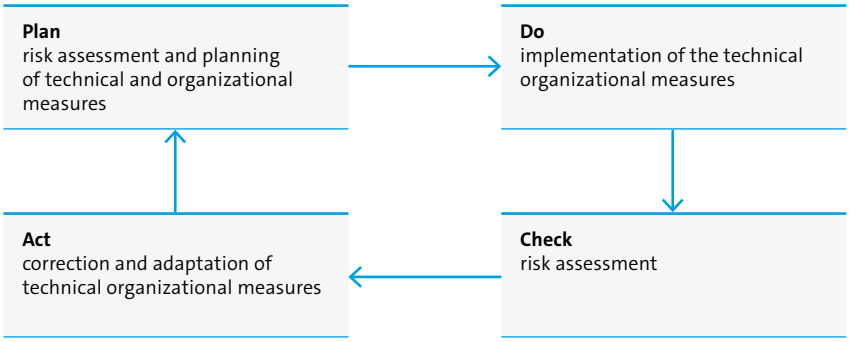


fig. 3: PDCA cycle

Due to the systematic proximity to the international standard DIN ISO / IEC 27001: 2015, which describes the requirements for an information security management system, as well as the thematic proximity of the security requirements for the processing of personal data to the fundamental security requirements of a company to the processing of all information, procedural and methodical merging of the two subject complexes is sensible. This does not only create significant synergies in the assessment and implementation of measures, it also increases the acceptance of the requirements in the company.

Comparison of the Requirements of DIN ISO/IEC 27001:2015 and GDPR

Phase in an ISMS	Article 32(1)(2) of the GDPR
risk assessment appropriate technical and organizational measures are to be taken incorporates: ▪ state of the art ▪ implementation costs ▪ nature, scope, context and purposes of the processing assessment standard (objectives): ▪ confidentiality ▪ integrity ▪ availability	"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk." (Article 32(1)(1) of the GDPR) "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed." (Article 32(2) of the GDPR)
A catalog of measures has to be developed, which meets at least the following criteria ▪ pseudonymization ▪ encryption ▪ confidentiality ▪ integrity ▪ availability ▪ fast BCM	"these measures include inter alia as appropriate": a) the pseudonymization and encryption of personal data b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (Article 32(1)(2)(a-c) of the GDPR)
internal audits and management review and Procedures for correction / adaptation of measures taken	"these measures include inter alia as appropriate": a) "a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing" (Article 32(1)(2)(d) GDPR)

4.3 Methods of ISO 27001 as Best-Practice

Proof of compliance with the requirement of an appropriate level of protection can be provided by means of various documentation which is usually accompanied is an ISMS according to ISO 27001:

- Overview of the assets (personal data / information and everything needed for its processing or which is required for it) - this may be / contain from the point of view of data protection, e.g. the processing records according to Article 30 of the GDPR (see ↗ Guideline "the Processing Records").
- determine technology for risk assessment
- risk management process
- risk identification, risk analysis and risk evaluation
- action plan
- risk management plan
- internal audit program and audit reports (including corrective measures)
- management report or report to the company management
- further documentation such as minutes from committee meetings, effectiveness tests, internal guidelines and specifications, training certificates etc.

The approach presented below provides a risk management procedure from a practical point of view:

4.4 Preliminary Considerations on the Implementation of "Security of Processing"

Organizations should introduce and run through a data protection risk management system by May 2018 for the individual business processes.

In preparation, two important considerations should be addressed and decided upon:

- Around what purpose or system is the risk assessment centered?
- How are risks assessed (methodology/technique)

The first question is important in order to be able to identify and allocate the risks according to a specific system or scheme. Regarding information security, the risks are allocated according to (information) assets – see for example DIN ISO / IEC 27001: 2015, which can be defined very differently. If one carries out a risk assessment which addresses only data protection, it is recom-

mended to map personal data in line with the processes. In these guidelines, processing activities are equated with business procedures. Depending on how detailed these are, processes can be either entire business processes or sub-processes.

In an integrated view, a reference to the associated processes is at least useful. Furthermore, groups of processes/assets can be combined or a two-step model can be used. In a two-step model, the company first identifies and evaluates the overall data protection risks for the entire data processing and determines a standard security level. In the second step, each procedure/asset is then examined to determine whether there are particular data protection risks of a specific procedure which require higher standards and additional necessary measures.

In addition to this basic structuring, it is important to define a risk assessment methodology or technique. This usually not only ensures that the threats and risks are viewed/determined systematically, but also ensures an assessment scale. This, in turn, is not only helpful for the people who have to carry out the assessment for the first time, but also creates a certain traceability and reproducibility. Only then, identified risks, including derived measures, fulfill the requirements of the accountability principle according to Article 5(1)(f) of the GDPR.

4.4.1 The Data Protection Risk Procedure

In principle, risk-related processes are very similar. A data protection risk procedure can be as follows:

- “Create the context” or “define the scope”
- Identifying risks
- Analyzing risks
- Evaluating risks
- Managing risks
- Monitoring risks

These six steps of risk management can be implemented very differently in practice depending on scope and used method. For example, the GDPR does not prescribe a method for risk analysis. Quantitative, qualitative methods or even mixed forms can be used to determine the measures to ensure an adequate level of protection. Even though only one method for risk analysis is used in this guide, this does not mean that other methods of risk analysis are not legally permitted.

4.4.2 Method of Risk Analysis

In the case of a classical risk analysis in information security, the risks are viewed with regard to a possible damage for the company. An extension of this information security risk analysis is possible but, according to the GDPR, the level of risk depends on its impact on data subjects. Therefore, a further perspective of interested parties has already been added to the procedural description.

An extension of the internal and external context is necessary so that the relevant risk criteria are also used to determine the risk level. "Likelihood" in information security is often presented as threats to the system, exploitable weaknesses, and the consequences of exploiting these weaknesses. Therefore, the focus lies upon the weakness of the system. This is different to the evaluation of the level of risk for data protection.

The level of data protection risk can be calculated as:

fig. 4: Risk Level

Although the primer goal is to protect the personal data of natural persons, this is only partly possible by information security measures. Instead, only the so-called supporting assets, e.g. hardware, software or network components, can be protected.

personal data = primary assets

Categories of supporting assets can be:[3]

- hardware and software of users
- hardware
- software
- data transmission channels
- individuals
- paper documents
- transmission of paper documents

3 ISO/IEC FDIS 29134:2017, Annex B.

Risk sources (people or nature) carry out actions against supporting assets. These actions, in turn, can lead to data breaches. The concrete scenario is called a threat.

Example:
Scenario: An employee (risk source) uses hardware on which personal data are processed (supported asset) contrary to the specific use (action). This means that personal data are lost (data protection risk). Concrete threat: An employee uses enterprise hardware for personal purposes.

4.5 Implementation "Security of Processing"

4.5.1 First Step: Involvement of Top Management

The involvement of top management (e.g. executive board, board of directors) is indispensable. In addition to the results of the risk evaluation, the risk treatment (in particular the risk acceptance) should also be coordinated or at least confirmed by top management. This also serves regularly to relieve the other employees. The results of the internal audits should also be regularly reported to the management.

In order to implement the accountability principle pursuant to Article 5 of the GDPR, regular minutes from committee meetings, effectiveness tests, internal guidelines and instructions as well as training certificates are recommended to be documented systematically and centrally.

4.5.2 Second Step: Defining Responsibilities

In order to be able to implement a DPIA, a corresponding project team must be equipped with the necessary competencies and resources by the management of the organization. Only if the management is committed to the implementation of a risk assessment, the introduction can be successful.

Operationally, this can be done, for example, by the adoption of a risk management policy that defines

- who is responsible for carrying out a risk assessment (security of processing and DPIA),
- who provides information and evaluates the data protection risks,
- how is the controller for data protection risks determined,

- how often is the business procedure carried out,
- what is the methodology/technique for risk assessment,
- which applicable risk treatment options are available,
- what happens with the analysis results of the security of processing and the DPIA.

4.5.3 Third Step: Defining the Internal and External Context

When considering the risks to the categories of data subjects, relevant data protection requirements (so called internal and external context) must be identified and taken into account during the risk assessment.

Data protection requirements can, for example, arise from:

- Requirements from international or national law
- Judicial decisions
- Regulations
- Contractual agreements (for example data processing on behalf of the controller)
- Business factors (for example codes of conduct, industry standards)
- Internal control systems (ICS)

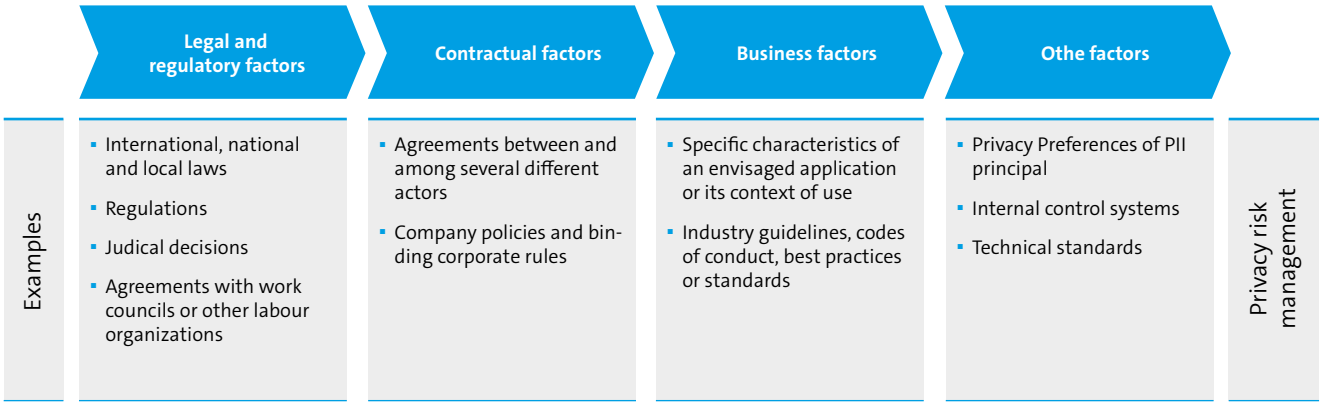


fig. 5: Data protection requirements from ISO/IEC 29100:2011, page 11

4.5.4 Fourth Step: Defining the Scope of the Analysis of "Security of Processing" (scoping)

In a first step, it is necessary to determine the scope for a risk assessment.

Subject-matter of a risk assessment can in principle be:

- business processes
- onetime actions or projects by the controller or
- IT infrastructure (software, hardware or network).

Here, it is a good idea to draw on a 'record of processing activities' as a basic structure, in case this already exists. The granularity of the record depends on practical aspects, such as the given instructions of a controller to a processor in the context of data processing on behalf (see ↗Bitkom Guideline on Processing Records). Hereinafter, one procedure is exemplarily described.

4.5.5 Fifth Step: Identification of Data Protection Risk

Data Protection Objectives to be Considered

In Article 32 of the GDPR only three (four) data protection objectives are considered:

- Availability (Resilience),
- Confidentiality and,
- Integrity.

Regarding the security of processing within the scope of risk assessment, it is only considered which risks entail a violation of the above-mentioned data protection objectives for data subjects.

The controller or the processer must identify the data protection risks that are inherent by the data processing activity. To identify risks, the following steps should classify risk sources, assets (including information, personal data, systems, etc.), threats and weaknesses, as well as possible impact and data protection risks. It is also useful to consider groups or to summarize similar assets. One possible approach is to use assets to derive the applicable data protection risks and thereby consider possible threats. This consideration can be carried out e.g. in interview form with relevant controllers, as well as in the form of workshops or brainstorming.

4.5.6 Sixth Step: Risk Analysis

First, existing measures to prevent the violation of confidentiality, availability or integrity are identified and documented.

It is irrelevant to the basic method whether and to what extent a company is already looking at a standard security level (in the sense of a two-step model) or looks at the procedure in isolation.

Example two-step risk assessment

A manufacturing, medium-sized company runs its IT completely on internal servers. The company operates exclusively in the B2B environment. In addition to the business contacts of current and future customers, the processing of personal data is limited to employee data. Based on a maximum principle, a risk assessment is carried out for processes taking types of data, affected categories of data subjects and amounts of data into account - thereby analyzing the entire IT and business environment. During the risk assessment, the maximum principle must be applied for each objective as mentioned above.

The result of the risk assessment shows that in the company's reintegration management (e.g. according to § 84(2) German SGB IX), much more sensitive data categories (health data of employees) are processed and therefore only a standard risk assessment is not sufficient.

Therefore, in a second step, the specific risks to data subjects for this specific procedure are considered and evaluated whether further measures are necessary.

Further triggers for a separate consideration could be, for example, the use of cloud services for individual processes, access by third parties to data, integration of service providers in third countries, etc.

Threats and Risk Sources

In this step, threats and their associated risk sources (triggering a threat) are determined.

Types of risk sources can be internal, external or even other sources (fire, water, natural disasters).

For the assessment of a risk source it can be helpful to know the internal or external motivation.

The following should be documented:

- Risk source (type)
- motivation

Then, threats are identified and assigned to the risk sources. This information is kept in a list.

Example for the Identification and Documentation of Risk Sources

Risk Sources (Type)			Relevant Risk Sources	Description of the Potency of Risk Sources
human risk source	internal	accidentally	employees, managers IT managers	Relevant sources of risk do not use resources for accidental actions.
		deliberately		Relevant sources of risk use minimal resources for deliberate actions (e.g.in the event of termination or warning).
	external	accidentally	IT managers, competitors, hackers	Relevant sources of risk do not use resources for accidental actions.
		deliberately		
non-human risk sources	internal		water damage due to pipe breakage, fire	Water damage due to pipe breakage and fire did not occur during the last 15 years of operation.
	external		power cut, Failure of internet connection	Failure of internet connection and power cut occur regularly, but the operational interruptions have not been relevant to date.

Impact on the violation of the three data protection objectives

The following three impacts are now to be considered in more detail:

- Unauthorized access to personal data
- Unwanted modification of personal data
- Loss of personal data

Now, the potential impacts in case of entry and the corresponding risk sources need to be attributed to the events:

Example for documentation and evaluation of incidents

Event (potential data protection incidents)	Risk Source	Result of entry of (adverse) event	Potential impact on interested parties
unauthorized access to personal data (confidentiality)	employees, supervisors, IT managers	▪ no further distribution ▪ use of personal data	Disclosure of payment data (bank data) from creditors and resulting monetary damages in case of misuse (damages).
unwanted alteration of personal data (integrity)	employees, supervisor, IT managers	▪ malfunction in process	liquidity problems of the organization
loss of personal data (availability)	employees, supervisors, IT managers, malicious code, water damage, fire	▪ malfunction in process ▪ disruption in process	liquidity problems of the organization

Identification of Relevant Risks

The relevant risk sources have already been identified. The following actions may now work on supported assets:

- Inappropriate use
- Monitoring
- Overload
- Manipulation
- Damage
- Alteration
- Loss

An overview of privacy impacts resulting from this can be found in annex B of ISO/IEC FDIS 29134:2017 or the “Knowledge base: Typology of threats” of the French Data Protection Authority, called CNIL[4]

4 CNIL, PIA Manual 2 - Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), 2015, p.18 ff.

Assessment of Severity of Impact

The impacts on the realization of a risk are, for example, first classified into four risk levels:

1. Negligible
2. Limited
3. Significant
4. Maximum

"The risk of the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to

- Physical
- Material or
- Non-material

damage."[5]

For each risk level, criteria and examples can be defined for the specific type of damage, which allow a classification and lead to the same results when a risk assessment is carried out again.

In order to make the results of the risk assessment repeatable, it is recommended to establish a classification system to assess the severity of impacts and also to be able to reuse them over and over again. An example of such a classification system can be found in the Annex "classification system". This proposal for a classification table came from the CNIL.

These categories can be adapted, if necessary, with existing categories and their criteria. Here, the law leaves the company flexibility to adequately define the method and adapt it to the company's situation. The choice of four levels for the assessment of the impact and the likelihood is common, but can be chosen differently depending on the business field of a company, the complexity of the processes or systems and many other factors.

5 Recital 75 of the GDPR.

Examples of the Impact Assessment from the Perspective of Different Interested Parties

First Case: Business Procedure "Production"

Scenario: A company operates a production of an economic asset. Not much personal data is processed during the production process. Protocols are kept in order to understand which employees were involved in the production at which time.

Assessment: A loss of these protocols has, for example, a "negligible" effect on the rights and freedoms of data subjects.

Second Case: Business Procedure "Internal Audit":

In order to carry out an internal audit, an internal auditor has to deal with a minimum of personal data, such as those of involved parties, responsibilities/roles.

Assessment: The disclosure of a protocol/report of an internal audit can be considered as "negligible" impact on the rights and freedoms of data subjects (data protection risk). However, from the company's perspective, the disclosure of a report of an internal audit can present a high risk, since trade secrets may be disclosed (monetary risk in the ISMS).

Third Case: Employment Agency for Celebrities

Scenario: An employment agency collects master data (address and contact details) from celebrities, in order to be able to connect people and write invoices.

Assessment: The disclosure of the celebrity's master data will be "significant" from the concerned data subject's perspective or even considered as "maximum". Although the GDPR does not classify address data as particularly sensitive, celebrities will have a special interest in the confidentiality of such data. Especially in the case of politicians or other officials, the protection of the address may be vital. In comparison, a simple assessment from the company's view could lead to a much lower risk assessment and thus not adequately reflect the requirements of the GDPR.

Assessment of the Likelihood

The likelihood takes into account many different aspects. In addition to the given circumstances (e.g. the location of a room with regard to the risk of water damage), business experience (number of comparable incidents in the past) and general statistics also play a role.

In a qualitative risk assessment, the likelihood can be divided into several stages. The law does not provide information on the number and evaluation of the stages. A potential raster for assessing the likelihood may for example look like this:

1. Negligible: It does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper document stored in a room protected by a badge reader and access code).
2. Limited: It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in a room protected by a badge reader).
3. Significant: It seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).
4. Maximum: It seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g. theft of paper documents stored in a public lobby).

4.5.7 Seventh Step: Risk Assessment

The following risk classes can arise out of the product of the effect and likelihood:

Risk classes	Factor
High risk	16
Risk	12-15
Reduced Risk	6-11
Low Risk	1-5

The GDPR refers to two risk levels “high risk” and “risk”, however, more risk levels can be introduced, as far as the user gains an advantage (e.g. gain more knowledge of information).

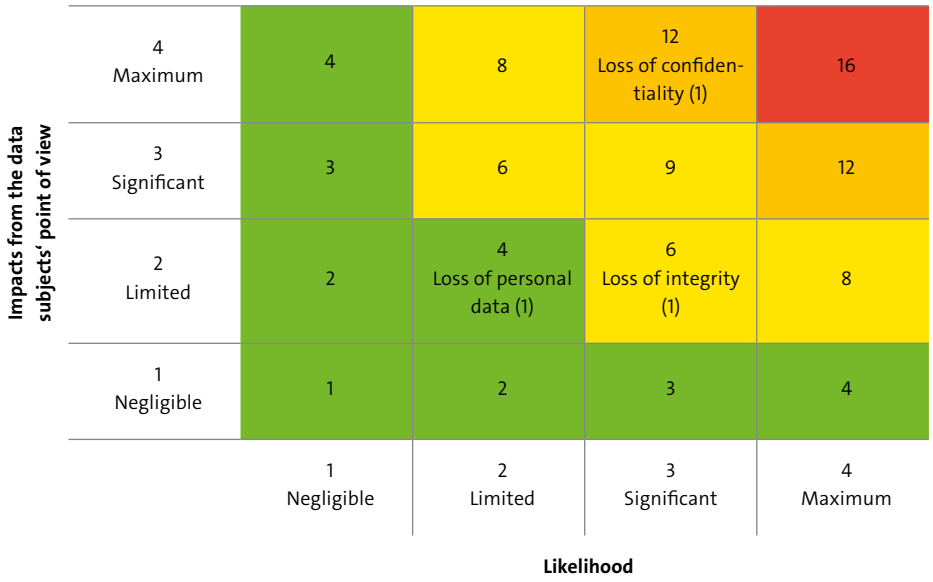
The classification of personal data into risk classes has an effect on the further use of this data, e.g

- If personal data is classified as high risk, it is important to check whether a DPIA needs to be carried out.
- If personal data were violated which belongs to the “risk” category, the competent supervisory authority must be notified.
- If personal data were violated which belongs to the “high risk” category, not only the competent authority but also the affected data subject needs to be informed.
- Exceptions to processing records according to Article 30 of the GDPR might no longer be applicable.

Risk Matrix to Present the Protection Level for the Respective Data Protection Risk

A representation of the risk as a product of likelihood and severity is possible in a risk matrix.

Example Risk Matrix with Four Levels



Calculated starting points for the risks of the data protection objectives availability, confidentiality and integrity are listed here in the risk matrix, with the asset with which they are currently available.

4.5.8 Eighth Step: Addressing Data Protection Risks

Overall there are four different ways to deal with risks:

- Risk reduction by taking measures
- Risk avoidance (e.g. by stopping to process certain categories of data)
- Risk transfer to third parties
- Risk acceptance

It is not always possible to use every of these risk reduction measures. For example, a risk transfer to third parties is often difficult to implement in data protection. Also, the risk acceptance, as far as the damage to the data subject is concerned, will not easily applicable.

Taking Measures

Article 32(1) of the GDPR only considers the option to reduce the level of risk by taking (data protection) measures.

In the case of a risk assessment, the law requires at least the implementation of the following measures

- Pseudonymization and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security o the processing.

In addition, Article 32 (4) requires from the controller and processer

- Access control
- Need-to-know-principle.

If risks are to be reduced by the taking measures, a corresponding list of measures should document

- Which measure is planned,
- Who is responsible for the implementation,
- By when it is planned to complete the implementation.

In addition, lists of measures can help the controller and processor in the planning phase to get an orientation.

List of Measures in Information Security and Data Protection

If measures for minimizing risk are to be taken, it is advisable to use commonly accepted measure lists. While many standards provide the user with comprehensive list of measures to minimize the risk, the application of a particular list is not required by law. The controller can choose a list of measures, provided that the aspects of Article 32(1)(2)(a-c) of the GDPR are taken into account.

For example, the following action measurement lists are used in information security:

- ISO/IEC FDIS 29151:2016: Guidelines on the protection of personal data,
- DIN ISO/IEC 27001:2015: Annex A and DIN ISO/IEC 27002:2016 as guideline for the interpretation of measures. In addition, sector-specific supplements of DIN ISO/IEC 27002:2016 can be used,
- Measurement list from the German Federal Office for Security in Information Technology (so called “BSI catalogues”).

For these lists, there are mapping tables for reconciliation[6] and they are thus compatible with each other. In the old German data protection law (BDSG) there has been an annex – so called Anlage zu §9 Satz 1 BDSG – which included certain technical and organizational measures in order to address specific privacy objectives (e.g. access control to data). Concrete measure for the implementation of risk-treatment controls are as proposed by literature.

There are also assignment tables for assigning information security measures to the risk-treatment goals of the BDSG.[7]

In order to avoid a fine, it is advisable to companies to use a generally recognized list of measures.

6 ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile.

7 ↗ http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/ErgaenzendeDoks/MassnahmeGS-Kat.pdf?__blob=publicationFile.

Data protection by Design and by Default

In addition to the use of

- Generic lists of measures,
- Existing approved codes of conduct,

the principles of data protection by design and default should also be taken into account and implemented, if possible.

Approved Codes of Conduct and Certification

The legislator probably had in mind that start-ups and SMEs will be regularly overwhelmed by the implementation of the aforementioned standards. Therefore, Article 32(3) of the GDPR explicitly points out that organizations can adhere to an approved code of conduct from associations or other organizations (Articles 40, 41 of the GDPR) and thereby demonstrate compliance with the security requirements of Article 32 of the GDPR. Likewise, the fulfilment of the requirements of data protection by design and default (Article 25 of the GDPR) can be demonstrated by certification in accordance with Article 42 of the GDPR.

Adherence to an approved code of conduct or certification mechanism could at the same time help the controller in implementing the GDPR. A successful and up-to-date certification according to Article 42 of the GDPR shall be taken into account by a competent authority when imposing a fine. However, please note that even an approved certification does not prevent an authority to look into the data protection practice of a company and enforce the law in case of non-compliance.

4.5.9 Ninth step: Monitoring and Review

The GDPR obliges the controller to establish and carry out a procedure to review and monitor the security of processing. Thereby, the effectiveness of the technical and organizational measures must be evaluated.

To fulfill the accountability duty of the GDPR, a detailed documentation of the planning (audit program) as well as the checks carried out (audit reports) is recommended.

If deviations are found in the audits, the remedies should also be systematized and documented.

4.6 Conclusion

To ensure the security of processing of controllers and processers under Article 32 of the GDPR, three points are desirable in the data protection practice:

1. Harmonized approaches for the analysis and implementation of the “security of processing” should be applied throughout the EU. Individualistic or experimental approaches for risk assessment should be avoided.

2. Good risk assessment procedures are those, which are well documented and can be also used by the average SME.

3. In order to address the risks with technical and organizational measures, well-documented and tested list of measures should be used to have a good reference point.

Once again, it should be pointed out that a data “protection risk” and a “risk in IT security” are not the same. For this reason, the security of processing according to Article 32 of the GDPR is not achieved by the simple use of an ISMS e.g. according to ISO/IEC 27001. However, it is possible to integrate both risk management systems up to a certain point. .

5 Data Protection Impact Assessment

5 Data Protection Impact Assessment

A data protection impact assessment widens the previous risk assessment view on the "security of data processing" by adding a view on the rights and freedoms of natural person and a compliance point of view. The latter one concerns compliance with legislative obligations. They comprise obligations the data subject can ask from the controller himself or via associations. Additionally the level of documentation is increased and – finally – the European legislator also recommends involving the data subject.

5.1 Checking the Obligation to Conduct a DPIA

Data protection authorities can establish a list of the kinds of processing activities for which, in general, no data protection impact assessment is required (whitelisting) and of the kinds of processing activities that are always subject to the requirement for a data protection impact assessment (blacklisting).

In certain cases the controller is obliged to conduct a data protection impact assessment. The severity of the interference with fundamental rights serves as orientation for the classification as a high risk for the rights and freedoms of the data subject. The GDPR demands that the controller assesses the data protection risk on the basis of objective criteria.

It is the view of the European legislator that especially new technologies are a trigger for the obligation to conduct a data protection impact assessment.

Irrespective of an obligation to conduct a data protection impact assessement, this can always be done voluntarily as addition to the risk assessment according to Article 32 of the GDPR.

As simplification of the procedure, several data processing activities with similarly high risks can be examined in one single assessment.

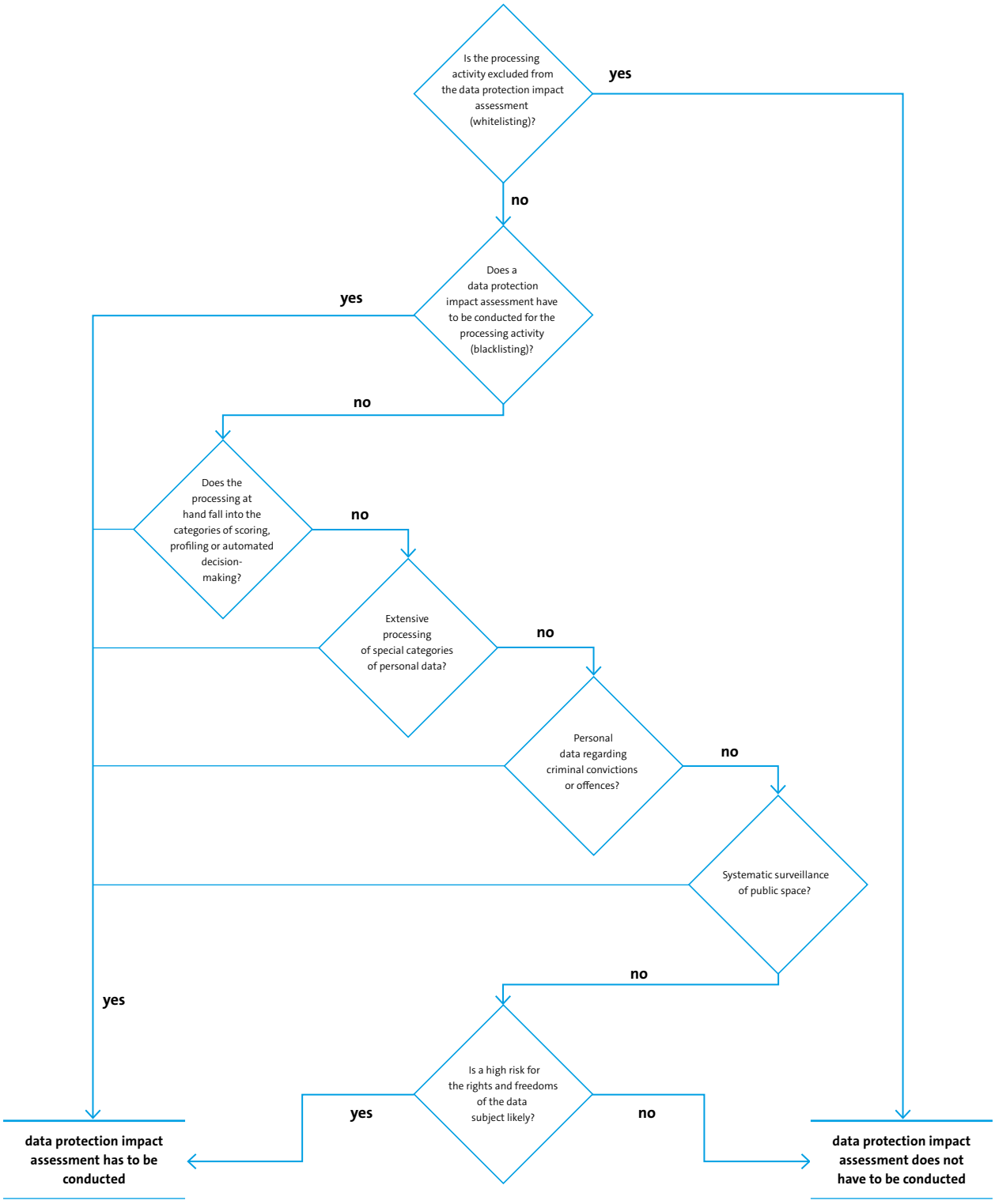

Is the processing activity excluded from the data protection impact assessment (whitelisting)?
yes
no
Does a data protection impact assessment have to be conducted for the processing activity (blacklisting)?
yes
no
Does the processing at hand fall into the categories of scoring, profiling or automated decision-making?
no
Extensive processing of special categories of personal data?
no
Personal data regarding criminal convictions or offences?
no
Systematic surveillance of public space?
no
yes
Is a high risk for the rights and freedoms of the data subject likely?
yes
no
data protection impact assessment has to be conducted
data protection impact assessment does not have to be conducted

fig. 6

5.2 The Role of the Data Protection Officer in the DPIA

If a data protection officer is appointed, he is only assisting the controller in an advisory capacity. It is not his task to initiate the DPIA, to undertake it by himself or assess the result. Therefore, it is recommended that e.g. for a substantial change in the information system of a company the change manager stays the owner of the project.

5.3 Description of the Purpose of the Data Processing

A description of the purposes of a certain data processing activity is already contained in the record of data processing activities. Therefore the parts that were already worked out should be used (see the invoicing example in Chapter 3 “Record of processing activities”).

Depending on the detail and accuracy of the description it will very probably be necessary to explain the legitimate interests of the controller.

Additionally, the controller has to assess the necessity and adequacy of the data processing activities in relation to the purpose.

5.4 Systematic Description of the Planned Data Processing Activities

In contrast to the security of the data processing, the processing activity has to be described in more detail in order to conduct a DPIA. For every phase of the processing the following aspects should be collected and documented:

Description of the steps of processing

- Information systems used
- Further supporting assets that are used

Depending on the processing phase within the life cycle of the data/information, the description can be done verbally in a table (see the following table as example) or as a data flow diagram in graphic form (see as example the following graphic from ISO/IEC FDIS 29134:2017). Other forms of description are also possible.

Example for a description of a processing activity (invoicing)

Phase of business process	Detailed Description of each phase	Information systems relevant for phase of process	Further supporting factors relevant for phase of process
Collection of personal data	Different departments mandate the invoice deprtment to prepare and send out offers. Master Data of interested parties and creditors are collected, if this hasn't happened before. Invoice data are collected.	Hardware: Desktop PCs, Application server (E-Mail and invoicing software), Fileserver Software: E-Mail-Server, E-Mail-Clients Invoicing software (Server) Invoicing software (Clients)	Accounting employees, Maintenance employees
Processing of personal data	Offers and invoices are prepared electronically and printed out in accounting department. Invoice data are corrected on request and resent. Master data of creditors are updated.	Hardware: Desktop PCs, Application server (E-Mail and invoicing software), Fileserver Software: E-Mail-Server, E-Mail-Clients Invoicing software (Server) Invoicing software (Clients)	Hard copies Accounting employees, Maintenance employees
Transfer of personal data	Printed offers and invoices are sent to interested parties and creditors per mail Monthly transfer of invoice data to financial accounts department.	Hardware: Desktop PCs, Application server (E-Mail and invoicing software), Fileserver Software: E-Mail-Server, E-Mail-Clients Invoicing software (Server) Invoicing software (Clients)	Hardcopies, Transfer via mail Accounting employees, Maintenance employees
Storage of personal data	Copies of sent out offers and invoices are kept as hardcopies in an archive room. Back up tapes of invoice data are stored for 10 years.	Hardware: Desktop PCs, Application server (E-Mail and invoicing software), Fileserver, Back up tapes Software: E-Mail-Server, E-Mail-Clients Invoicing Software (Server) Invoicing-Software (Clients)	Hard copies Accounting employees, Maintenance employees
Elimination of personal data	Data storage media are destroyed, when the data storage medium has reached its maximum Life span minus a security span or when the maximum storage time of the personal data on the storage medium has been reached.	Hardware: Desktop PCs, Application server (E-Mail and invoicing software), Fileserver, Back up tapes Software: E-Mail-Server, E-Mail-Clients	Accounting employees, Destroyer of data storage media

The result of a detailed description of a processing activity can also be a data flow diagram:

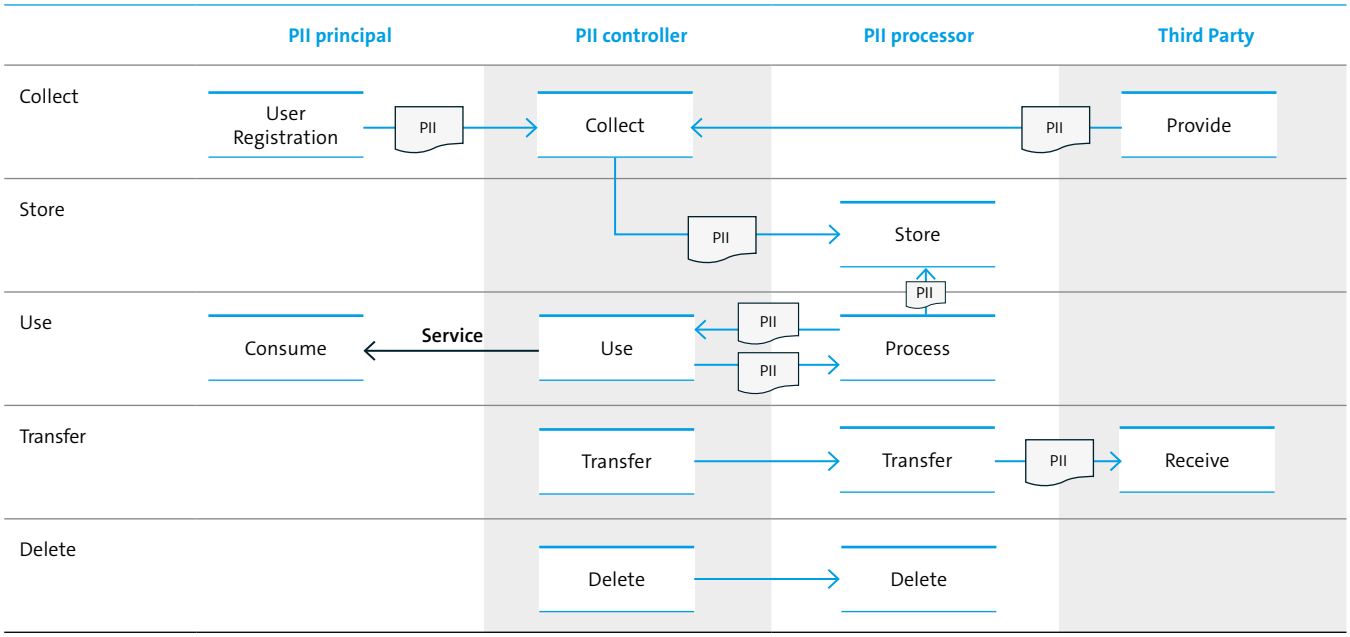


fig. 7: ISO/IEC FDIS 29134:2017, Page 40

5.5 Assessment of Risks for the Rights and Freedoms of the Data Subject

The GDPR stands for a number of data protection principles and names the majority of them in Article 5 of the GDPR.

Data Protection Principles[8]	Data Protection Risk: Violation of rights and freedoms of natural persons	Compliance-Risk: Violations of the GDPR	Information Security Risk: Violation of principles of information security
1. Lawfulness and fairness	Article 5(1)(a)	Article 6(1)(a)Consent Article 6(1)(b)Contract with the data subject or legal obligation Article 6(1)(c) necessary for compliance with a legal obligation Article 6(1)(d) vital interests of the data subject Article 6(1)(e) public interest Article 6(1)(f) legitimate interest of controller or third party Article 21 Right to object Article 22 Right not to be subject to solely automated decisions	

8 The data protection principles are explained in annex 6.

Data Protection Principles[8]	Data Protection Risk: Violation of rights and freedoms of natural persons	Compliance-Risk: Violations of the GDPR	Information Security Risk: Violation of principles of information security
2. Transparency	Article 5(1)(a)	Article 12 Modalities for the exercise of the rights of the data subject Article 13 Information at collection from the data subject Article 14 Information at collection of data somewhere else Article 15 Right of Access	
3. Purpose limitation	Article 5(1)(b)	Article 6(4) Compatible purpose Article 13(3 und Article 14(4) Information on compatible purpose	
4. Data minimization	Article 5(1)(c)	Article 25 Data Protection by Design and by Default Article 17 Right to erasure	
5. Accuracy	Article 5(1)(d)	Article 16 Right to rectification	
6. Storage limitation	Article 5(1)(e)	Article 17 Right to erasure Article 18 Right to restriction of processing	
7. Integrity and confidentiality	Article 5(1)(f)	Article 34 Communication of a breach	Article 32(1)(b) Ensure the ongoing confidentiality and integrity
8. Availability (resilience)			Article 32(1)(b) Ensure the ongoing availability and resilience Article 32(1)(c) restore access to data in a timely manner
9. Personal participation and access		Article 16 Right to rectification Article 17 Right to erasure Article 18 Right to restriction of processing Article 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing Article 20 Right to data portability	
10. Accountability	Article 5(2) Accountability	Article 30 Record of processing activities Article 32 Security of processing Article 35 Data protection impact assessment Article 36 Prior consultation	

8 The data protection principles are explained in annex 6.

The controller has to describe which data protection risks might arise for the data subject in case of a violation of data protection principles.

The information security point of view has already been elaborated in Chapter “Security of Processing” and can be transferred to the data protection impact assessment.

Example: Video Surveillance in the Entrance Area of a Company
Employees have access to the company building via several entrances. Employees access the building via a man trap. The authentication is done via chip cards. Only the main entrance has security personnel. The security personnel can see the side entrances with the help of video cameras (only extended eye view) , the faces of persons can be identified on the screen. Security personnel only uses this possibility if requested by an employee (who has a problem with the man trap) or by accident, to check whether the man traps are circumvented.

Begin of Assessment

An assessment is only needed, when it has been confirmed that personal data are collected, processed or used.

As people’s faces can be identified, personal data are collected.

Compliance-View

The compliance view contains several data protection principles that have to be assessed. An assessment comprises the complete life cycle of personal data, if the processing phases are relevant.

Excursus: Phases of Processing:

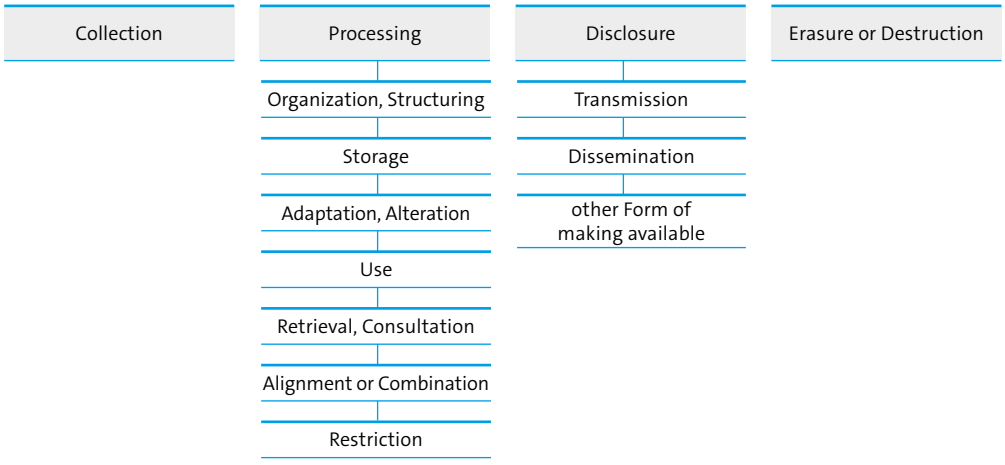


fig. 8: Phases of Processing

Assessment of Data Protection Principles

Compliance-View	
1 Lawfulness and Fairness of Data Processing A video surveillance of the side entrances is allowed under Art. 6 (1)(f) of the GDPR.	**10 Accountability** The data protection measures are enforced by the controller, the measures are adequate to the risk, there are processes to deal with incidents and a chain of information, the data protection measures are monitored regularly, Data protection responsibilities are determined by the controller, data protection is built in the company wide governance system
2 Transparency Measure: The video surveillance is marked with adherence to the requirements of Article 13 of the GDPR.	
3 Purpose Limitation The video surveillance may only be used by the security personnel to support the employees or for random sample control of possible circumvention of man traps. As an alternative to the video surveillance (extended eye) one had to post security personnel at every side entrance, which with regard to the existing risk for the rights and freedoms of the data subjects seems disproportionate in comparison to the costs. In a survey where the data subjects were asked about the closure of side entrances as compromise for a cost neutral design of the entrance situation they declined this proposal with overwhelming majority of the employees. (´Assessment of risks for the rights and freedoms of data subjects according to Article 35(7)(c)	
4 Data Minimization Measure: The cameras are adjusted in a way that only the relevant region of the man trap is captured. (Passepartout or Blurring) .	
5 Accuracy Measure: As no personal data is stored or disclosed, no erasure or correction concept is needed.	
6 Storage Limitation Measure: As no personal data is stored or disclosed, no erasure or correction concept is needed.	
9 Personal Participation and Access Measure: Data subjects can ask the responsible person of the security personnel directly for general information on the video surveillance or ask the data protection officer. .	

Result:

1. The data protection principles of the compliance view are fulfilled.
2. Taking into account the described measures the data protection risk analysis does not show a high risk for the rights and freedoms of the data subjects.

5.6 The Measures Planned to Address Risks

The controller has to describe which measures he will put in place in order to avoid violations of the data protection principles. Again we have to differentiate between the compliance and the security of information point of view.

In Article 35(7)(d), the GDPR particularly requires the determination of measures (including guarantees, security measures and processes) that ensure the protection of personal data and that prove the fulfillment of the GDPR requirements. The rights of data subjects and other affected subjects have to be taken into account.

	There **is no approved Code of Conduct** available for the processing activity.		There **is an approved Code of Conduct** available for the processing activity.
	Possible catalogue of measures by CNIL: CNIL, Measures for the privacy risk treatment, 2012	To pay attention to when technology is used:	In case the organization wants to submit to an approved code of conduct
Compliance View	Possible catalogues of measures from ISO Family: For Controllers: ISO/IEC DIS 29151, Annex A For Processors: ISO/IEC 27018, Annex A	Data Protection by Design and by Default, Article 25 of the GDPR	Application of approved code of conduct
Risk View	Possible catalogue of measures by CNIL: CNIL, Measures for the privacy risk treatment, 2012 Possible catalogues of measures from ISO Family: For Controllers: ISO/IEC DIS 29151, Annex A For Processors: ISO/IEC 27018, Annex A With the explanations of ISO/IEC 27002		

If an organization decides to take measures in order to address data protection risks, for accountability reasons it is advisable to put these measures for minimizing data protection risks in a measurement list and determine a deadline and someone who is responsible for each measure. In risk management such a list is also called risk management plans.

No approved codes of conduct exist

The compliance view comprises legally binding measures. These measures have to be implemented.

> **Example:** A processing activity can only be legal or illegal – being a little legal or illegal is not possible.

Measures for the compliance with data protection principles are contained for example in ISO/IEC FDIS 29151:2016 Annex A, DIN ISO/IEC 27018:2014 Annex A (for processors) or also in papers of the CNIL.

The risk view comprises measures that result from a risk assessment.

> **Example:** Admission to a building can be prevented through many different measures: Door lock, alarm system, security personnel, etc.

For the determination of measures in this field one can look into the measures from ISO-catalogues (ISO/IEC FDIS 29151:2016, ISO/IEC 27018:2014, DIN ISO/IEC 27002:2016) or use the building blocks of the "IT-Grundschutz-catalogues" from the German BSI.

Approved Codes of Conduct exist

If there are approved codes of conduct for the actual situation that has to be assessed, they should be used before going back to general catalogues of measures.

Data Protection by Design and by Default

When using technology one should always make sure that the principles of data protection by design and by default are considered.

5.7 Role of Interested Parties

While during an analysis of the security of the processing the risk assessment has to be done from a point of view of the data subject, the involvement of interested parties is also explicitly foreseen for a data protection impact assessment, but not strictly prescribed ("where appropriate").

Even if the involvement of interested parties can lead to high costs, one should consider the involvement, as this involvement could create acceptance through transparency and this could be in the controller's own interest. It should also be kept in mind that the data subject's appetite to take risks is usually not assessed correctly from the companies' perspective.

5.8 DPIA Report

A report for a data protection impact assessment must contain at least the following elements according to Article 35(7) of the GDPR:

- A systematic description of the planned processing activities and of the purposes of the processing, inclusive the legitimate interests of the controller (if applicable);
- an assessment of the necessity and adequacy of the data processing activities in relation to the purpose;
- an assessment of the risks for the rights and freedoms of the data subjects according to paragraph 1 and
- the measures that are planned in order to address existing risks, including guarantees, security measures and processes, that ensure the protection of personal data and that prove the fulfillment of the GDPR requirements and whereupon the rights of data subjects and other affected subjects are taken into account.

If a consultation of the data protection supervisory authority is necessary, the DPIA report has to be amended by the following information (Article 36(3) of the GDPR):

- if applicable, information on the respective responsibilities of the controller, the joint controller and the involved data processors, especially when the processing takes place in a group of companies;
- purposes and means of the planned data processing activity;
- the measures and guarantees foreseen for the protection of the rights and freedoms of data subjects by the GDPR;
- if applicable the contact details of the data protection officer;
- data protection impact assessment according to Article 35 of the GDPR and
- all other information requested by the data protection supervisory authority.

One possible structure for a data protection impact assessment report that fulfills the requirements of Article 35(7) of the GDPR could look like this:

Data Protection Impact Assessment

1 Introduction

2 Scope of data protection impact assessment
- 2.1 Systematic description of purposes of the data processing activities
- 2.2 Assessment of necessity and adequacy of processing activities in relation to the purpose
- 2.3 Purposes and means of the planned processing
- 2.4 Parties involved:
  - 2.4.1 Controller
  - 2.4.2 Joint Controllers
  - 2.4.3 Processor(s)
  - 2.4.4 Contact Data Protection Officer

3 Data protection Requirements

4 Data protection Risk Perspective
- 4.1 Data protection risk identification
- 4.2 Data protection risk analysis
- 4.3 Data protection risk assessment

5 Planned measures, including guarantees, security measures and processes that ensure the protection of personal data as well as proof of protection.

6 Result of data protection impact assessment and possible obligation to consult the data protection authority

5.9 Consultation Process

If there is still a high risk for the rights and freedoms of the data subject after measures have been taken to reduce the risks (“in the absence of measures by the controller” and “and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation”), the controller has to consult the supervisory authority before the data processing starts. The controller provides the supervisory authority for the consultation with the information described in Chapter 5.8.B

During the consultation process, the supervisory authority checks whether the processing in question is compliant with the GDPR. If this is not the case, the controller is informed within 14 weeks (maximum 8 weeks and a possible extension of 6 weeks). In case of compliance, the GDPR does not require a notification of the supervisory authority.

6 Annex

Criteria that should be considered according to the Art. 29 Working Party (WP 248) when identifying a high risk (that requires the undertaking of a DPIA)

On p. 7-10 of WP 248 the Art. 29 Working Party lists criteria that should be considered when asking whether a DPIA is necessary. The Working Party assumes that the more criteria are fulfilled at the same time the more probable is a high risk for the rights and freedoms of the data subjects

1. Evaluation or scoring, including profiling and predicting
2. Automated-decision making with legal or similar significant effect
3. Systematic monitoring
4. Sensitive data
5. Data processed on a large scale
6. Datasets that have been matched or combined
7. Data concerning vulnerable data subject
8. Innovative use or applying technological or organizational solutions
9. Data transfer across borders outside the European Union
10. When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and Recital 91)

Table for Classification of Risks

As an example we use the proposal from CNIL as a table for the evaluation of the severity of the effect of the processing[10]

Levels	1. Negligible	2. Limited	3. Significant	4. Maximum
Generic description of impacts (direct and indirect)	▪ Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.	▪ Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties	▪ Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties	▪ Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome

10 CNIL, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases), 2015, Seite 13 ff.

Levels	1. Negligible	2. Limited	3. Significant	4. Maximum
Examples of physical impacts	▪ Lack of adequate care for a dependent person (minor, person under guardianship) ▪ Transient headaches	▪ Minor physical ailments (e.g. minor illness due to disregard of contraindications) ▪ Lack of care leading to a minor but real harm (e.g. disability) ▪ Defamation resulting in physical or psychological retaliation	▪ Serious physical ailments causing long-term harm (e.g. worsening of health due to improper care, or disregard of contraindications) ▪ Alteration of physical integrity for example following an assault, an accident at home, work, etc.	▪ Long-term or permanent physical ailments (e.g. due to disregard of contraindications) ▪ Death (e.g. murder, suicide, fatal accident) ▪ Permanent impairment of physical integrity
Examples of material impacts	▪ Loss of time in repeating formalities or waiting for them to be fulfilled ▪ Receipt of unsolicited mail (e.g. spams) ▪ Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing) ▪ Targeted advertising for common consumer products	▪ Unanticipated payments (e.g. fines imposed erroneously), additional costs (e.g. bank charges, legal fees), payment defaults Denial of access to administrative services or commercial services ▪ Lost opportunities of comfort (i.e. cancellation of leisure, purchases, holiday, termination of an online account) ▪ Missed career promotion ▪ Blocked online services account (e.g. games, administration) ▪ Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects ▪ Cost rise (e.g. increased insurance prices) ▪ Non-updated data (e.g. position held previously) ▪ Processing of incorrect data creating for example accounts malfunctions (bank, customers, with social organizations, etc.) ▪ Targeted online advertising on a private aspect that the individual wanted to keep confidential (e.g. pregnancy advertising, drug treatment) ▪ Inaccurate or inappropriate profiling	▪ Misappropriation of money not compensated ▪ Non-temporary financial difficulties (e.g. obligation to take a loan) ▪ Targeted, unique and nonrecurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban) ▪ Prohibition on the holding of bank accounts ▪ Damage to property ▪ Loss of housing ▪ Loss of employment ▪ Separation or divorce ▪ Financial loss as a result of a fraud (e.g. after an attempted phishing) ▪ Blocked abroad ▪ Loss of customer data	▪ Financial risk ▪ Substantial debts ▪ Inability to work ▪ Inability to relocate ▪ Loss of evidence in the context of litigation ▪ Loss of access to vital infrastructure (water, electricity)

Levels	1. Negligible	2. Limited	3. Significant	4. Maximum
Examples of moral impacts	▪ Mere annoyance caused by information received or requested ▪ Fear of losing control over one's data ▪ Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion) ▪ Loss of time in configuring one's data ▪ Lack of respect for the freedom of online movement due to the denial of access to a commercial site (e.g. alcohol because of the wrong age)	▪ Refusal to continue using information systems (whistleblowing, social networks) ▪ Minor but objective psychological ailments (defamation, reputation) ▪ Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation, loss of recognition) ▪ Feeling of invasion of privacy without irreversible damage ▪ Intimidation on social networks	▪ Serious psychological ailments (e.g. depression, development of a phobia) ▪ Feeling of invasion of privacy with irreversible damage ▪ Feeling of vulnerability after a summons to court ▪ Feeling of violation of fundamental rights (e.g. discrimination, freedom of expression) ▪ Victim of blackmailing ▪ Cyberbullying and harassment	▪ Long-term or permanent psychological ailments ▪ Criminal penalty ▪ Abduction ▪ Loss of family ties ▪ Inability to sue ▪ Change of administrative status and/or loss of legal autonomy (guardianship)

Data Protection Principles

Compliance View	
1 Lawfulness of Data Processing and Fair Processing (processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")); Article 5(1)(a) of the GDPR Recital 39: Any processing of personal data should be lawful and fair.	**10 Accountability** The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability"); Article 5(2) of the GDPR.
2 Transparency (Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")); Article 5(1)(a) of the GDPR Recital 39: It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing Measure taken: An designation of the video surveillance is carried out taking into account the requirements of the Article 13 GDPR.	

3 Purpose Limitation
(Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation")); Article 5(1)(b) of the GDPR

Recital 39: In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. [...] Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

4 Data Minimization
(Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"); Article 5(1)(c) of the GDPR

Recital 39: The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed..

5 Storage Limitation
(Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")); Article 5(1)(e) of the GDPR

Recital 39: This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. [...] In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

6 Accuracy
(Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy")); Article 5(1)(d) of the GDPR.

Recital 39: Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted.

7 Participation and Access

10 Accountability
The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability"); Article 5(2) of the GDPR.

Risk View

8 Integrity and Confidentiality
(Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality"); Article 5(1)(f) of the GDPR

Recital 39: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing.

9 Availability (and Resilience);
Article 32(1)(b) of the GDPR

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability").

Catalogue of Data Protection Measures of CNIL

The CNIL gives an overview on data protection measures. The different measures are explained in PIA Manual 3 of CNIL. As this catalogue was written before the GDPR, the legal requirements have to be added to the requirements of the CNIL. The other blocks can be taken as they are.

1. Legal controls (mandatory)	
Purpose: specified, explicit and legitimate purpose	Data
Minimization: limiting the amount of personal data to what is strictly necessary	Data
Quality: preserving the quality of personal data	Data
Retention periods: period needed in order to achieve the purposes, in the absence of another legal obligation imposing a longer retention period	Data
Information: respect for data subjects' right to information	Data
Consent: obtaining the consent of data subjects or existence of another legal basis justifying the processing of personal data	Data
right to object: respect for the data subjects' right to object	Data
Right of access: respect for data subjects' right to access their data	Data
Right to rectification: respect for data subjects' right to correct their data and erase them	Data
Transfers: compliance with obligations relating to transfer of data outside the European Union	Data
Prior checking: definition and fulfillment of formalities prior to processing	Data

2. Organizational controls	
Organization	Cross-organizational
Policy (management of rules)	Cross-organizational
Risk management	Cross-organizational
Project management	Cross-organizational
Management of incidents and data breaches	Impacts
Staff management	Sources
Relationships with third parties	Sources
Maintenance	Sources
Supervision (audits, dashboards, etc.)	Cross-organizational
Marking of documents	Sources
Archival	Cross-organizational

3. Logical security controls	
Anonymization	Data
Encryption	Sources
Integrity checks	Impacts
Backups	Impacts
Data partitioning	Sources
Logical access control	Sources
Traceability	Sources
Operations	Supporting assets
Monitoring (settings, configuration controls, real-time monitoring, etc.)	Supporting assets
Workstation management	Supporting assets
Fight against malicious code (viruses, spyware, software bomb, etc.)	Sources
Protection of computer channels (networks)	Supporting assets

4. Physical security controls	
Distancing of risk sources (dangerous products, dangerous geographic areas, etc.)	Sources
Physical access control	Sources
Security of hardware	Supporting assets
Security of paper documents	Supporting assets
Security of paper channels	Supporting assets
Protection from non-human risk sources (fire, water, etc.)	Sources

Catalogue of Controls from ISO/IEC DIS 29151

ISO/IEC FDIS 29151:2016 proposes an extended catalogue of controls to the user.

A.1 General policies for the use and protection of PII

A.2 Consent and choice
- A.2.1 Consent
- A.2.2 Choice

A.3 Purpose legitimacy and specification
- A.3.1 Purpose legitimacy
- A.3.2 Purpose specification

A.4 Collection limitation
- A.4.1 Collection limitation

A.5 Data minimization
- A.5.1 Minimization

A.6 Use, retention and disclosure limitation
- A.6.1 Use, retention and disclosure limitation
- A.6.2 Secure erasure of temporary files
- A.6.3 PII disclosure notification
- A.6.4 Recording of PII disclosures
- A.6.5 Disclosure of sub-contracted PII processing

A.7 Accuracy and quality
- A.7.1 Data quality

A.8 Openness, transparency and notice
- A.8.1 Privacy notice
- A.8.2 Openness and transparency

A.9 PII principal participation and access
- A.9.1 PII principal access
- A.9.2 Redress and participation
- A.9.3 Complaint management

A.10 Accountability

- A.10.1 Governance
- A.10.2 Privacy risk assessment
- A.10.3 Privacy requirement for contractors and PII processors
- A.10.4 Privacy monitoring and auditing
- A.10.5 PII protection awareness and training
- A.10.6 PII protection reporting

A.11 Information security

A.12 Privacy compliance

- A.12.1 Compliance
- A.12.2 Cross border data transfer restrictions in certain jurisdictions

5 Information security policies

- 5.1 Management directions for information security
  - 5.1.1 Policies for information security

6 Organization of information security

- 6.1 Internal organization
  - 6.1.1 Information security roles and responsibilities
  - 6.1.2 Segregation of duties
  - 6.1.3 Contact with authorities
  - 6.1.4 Contact with special interest groups
  - 6.1.5 Information security in project management
- 6.2 Mobile devices and teleworking

7 Human resource security

- 7.1 Prior to employment
- 7.2 During employment
  - 7.2.1 Management responsibilities
  - 7.2.2 Information security awareness, education and training
  - 7.2.3 Disciplinary process
- 7.3 Termination or change of employment

8 Asset management

9 Access control

- 9.1 Business requirement of access control
- 9.2 User access management
  - 9.2.1 User registration and de-registration
  - 9.2.2 User access provisioning
  - 9.2.3 Management of privileged access rights
  - 9.2.4 Management of secret authentication information of users

  - 9.2.5 Review of user access rights
  - 9.2.6 Removal or adjustment of access rights
- 9.3 User responsibilities
  - 9.3.1 Use of secret authentication information
- 9.4 System and application access control
  - 9.4.1 Information access restriction
  - 9.4.2 Secure log-on procedures
  - 9.4.3 Password management system
  - 9.4.4 Use of privileged utility programs
  - 9.4.5 Access control to program source code

10 Cryptography

- 10.1 Cryptographic controls
  - 10.1.1 Policy on the use of cryptographic controls
  - 10.1.2 Key management

11 Physical and environmental security

- 11.1 Secure areas
- 11.2 Equipment
  - 11.2.1 Equipment siting and protection
  - 11.2.2 Supporting utilities
  - 11.2.3 Cabling security
  - 11.2.4 Equipment maintenance
  - 11.2.5 Removal of assets
  - 11.2.6 Security of equipment and assets off-premises
  - 11.2.7 Secure disposal or re-use of equipment
  - 11.2.8 Unattended user equipment
  - 11.2.9 Clear desk and clear screen policy

12 Operations security

- 12.1 Operational procedures and responsibilities
  - 12.1.1 Documented operating procedures
  - 12.1.2 Change management
  - 12.1.3 Capacity management
  - 12.1.4 Separation of development, testing and operational environments
- 12.2 Protection from malware
- 12.3 Backup
  - 12.3.1 Information backup
- 12.4 Logging and monitoring
  - 12.4.1 Event logging
  - 12.4.2 Protection of log information
  - 12.4.3 Administrator and operator logs
  - 12.4.4 Clock synchronization
- 12.5 Control of operational software

- 12.6 Technical vulnerability management
- 12.7 Information systems audit considerations

13 Communications security

- 13.1 Network security management
- 13.2 Information transfer
  - 13.2.1 Information transfer policies and procedures
  - 13.2.2 Agreements on information transfer
  - 13.2.3 Electronic messaging
  - 13.2.4 Confidentiality or non-disclosure agreements

14 System acquisition, development and maintenance

15 Supplier relationships

16 Information security incident management

- 16.1 Management of information security incidents and improvements
  - 16.1.1 Responsibilities and procedures
  - 16.1.2 Reporting information security events
  - 16.1.3 Reporting security weaknesses
  - 16.1.4 Assessment of and decision on information security events
  - 16.1.5 Response to information security incidents
  - 16.1.6 Learning from information security incidents
  - 16.1.7 Collection of evidence

17 Information security aspects of business continuity management

18 Compliance

- 18.1 Compliance with legal and contractual requirements
- 18.2 Information security reviews
  - 18.2.1 Independent review of information security
  - 18.2.2 Compliance with security policies and standards
  - 18.2.3 Technical compliance review

Bitkom represents more than 2,600 companies in the digital sector, including 1,600 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom´s members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

Bitkom e.V.
Federal Association for Information Technology, Telecommunications and New Media

Albrechtstraße 10
10117 Berlin
T +4930 27576-0
F +4930 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom