

Nicholas Martin, Michael Friedewald, Ina Schiering, Britta A. Mester, Dara Hallinan, Meiko Jensen

# THE DATA PROTECTION IMPACT ASSESSMENT ACCORDING TO ARTICLE 35 GDPR

A Practitioner's Manual



### Contact

Fraunhofer Institute for Systems and Innovation  
Research ISI  
Breslauer Strasse 48  
76139 Karlsruhe  
Phone +49 721 6809-0  
Fax +49 721 68 09-176  
E-Mail [info@isi.fraunhofer.de](mailto:info@isi.fraunhofer.de)  
URL [www.isi.fraunhofer.de](http://www.isi.fraunhofer.de)

### Typographic design and graphics

scientific design gbr, Neustadt an der Weinstrasse

### Cover photo

Composing: Stefanie Ziegler, photo: © bannosuke/  
fotolia, pictogram (couple): © pixabay

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

The work underlying this publication was supported by the Germany Federal Ministry of Education and Research, under the grant numbers 03VP03551, 03VP03552 and 03VP03553. Responsibility for the contents of this publication lies solely with the authors.



This work is licensed under a creative commons attribution 4.0 international license.

Martin, N., Friedewald, M. et al.: The Data Protection Impact Assessment according to Article 35 GDPR. A Practitioner's Manual. Stuttgart: Fraunhofer Verlag 2020.

# THE DATA PROTECTION IMPACT ASSESSMENT ACCORDING TO ARTICLE 35 GDPR

## A Practitioner's Manual

Authors:

**Nicholas Martin, Michael Friedewald, Ina Schiering,  
Britta A. Mester, Dara Hallinan, Meiko Jensen**

Editors:

Michael Friedewald and Nicholas Martin  
Fraunhofer Institute for Systems and Innovation Research ISI  
Karlsruhe

---

**In cooperation with**

 **FIZ Karlsruhe**  
Leibniz-Institut für Informationsinfrastruktur

 **Fachhochschule Kiel**  
University of Applied Sciences

 **Ostfalia**  
Hochschule für angewandte  
Wissenschaften

**datenschutz**  **nord**

# TABLE OF CONTENTS

<b>ACKNOWLEDGEMENTS</b>	<b>4</b>
<hr/>	
<b>SUMMARY DATA PROTECTION IMPACT ASSESSMENT</b>	<b>5</b>
<hr/>	
<b>A PRACTICAL APPROACH TO DPIA</b>	<b>13</b>
<b>1 Introduction</b>	<b>13</b>
1.1 Data protection	13
1.2 Data protection impact assessment	15
1.3 Responsibility for the DPIA	16
Controller	16
Data protection officer	17
Product producers, processors, and joint controllers	18
<b>2 Necessary preliminary work</b>	<b>20</b>
2.1 Records of processing activities according to Article 30 GDPR	20
2.2 Stakeholders	21
2.3 Documentation of the legal basis of processing	21
2.4 Assessing the necessity and proportionality of processing	22
<b>3 DPIA phases</b>	<b>23</b>
<b>4 Phase I: Initiation of the DPIA</b>	<b>25</b>
4.1 Approach	25
4.2 Reviewing the requirements of Article 35(3) GDPR	26
4.3 Lists of the data protection supervisory authorities	27
4.4 Criteria of Article 29 Data Protection Working Party	28
4.5 Independent review	28
4.6 Documentation of the result	29
<b>5 Phase II: Preparation of the DPIA</b>	<b>30</b>
5.1 Approach	30
5.2 Collection of information and description of the processing operations and the purposes of the processing	30
5.3 Identification of the data subjects	32
5.4 Identification of other stakeholders	33
5.5 DPIA team	35

<b>6</b>	<b>Phase III.: Execution of the DPIA</b>	<b>37</b>
6.1	Method	37
6.2	What are risks as defined in the GDPR?	37
	Damages and interference with rights and freedoms	38
	Events	40
6.3	Risk assessment using the protection goals and damage scenarios	40
	Creating damage scenarios	42
	Analysis based on the data protection goals	44
6.4	Risk assessment	45
6.5	Selection of mitigation measures	46
6.6	Assessment of the remaining risks and decision about further steps	47
6.7	Assessment of necessity and proportionality	48
6.8	Recommended method: Participatory workshop-based method	48
6.9	DPIA report	49
6.10	Prior consultation of the supervisory authorities	50
<b>7</b>	<b>Phase IV: Implementation of the DPIA</b>	<b>51</b>
7.1	Implementing and testing the mitigation measures	51
7.2	Demonstrating compliance with the GDPR and approval of the processing	51
<b>8</b>	<b>Phase V: Periodic review of the DPIA</b>	<b>52</b>
<hr/>		
	<b>APPENDIX</b>	<b>53</b>
<b>A</b>	<b>Description of the protection goals</b>	<b>53</b>
A.1	Data minimization	53
A.2	Availability	55
A.3	Integrity	56
A.4	Confidentiality	57
A.5	Unlinkability	58
A.6	Transparency	58
A.7	Intervenability	60
<b>B</b>	<b>Further literature</b>	<b>62</b>
<b>C</b>	<b>Abbreviations</b>	<b>63</b>
<b>D</b>	<b>Footnotes</b>	<b>64</b>
<b>E</b>	<b>About the authors</b>	<b>66</b>

## ACKNOWLEDGEMENTS

This handbook operationalizes an approach to data protection impact assessments that was introduced in a White Paper by the research consortium *Forum Privacy and Self-Determination in a Digital World*.<sup>1</sup>

The basis for operationalizing and further developing the approach were twelve workshops and interviews with enterprises and public authorities. These were conducted in 2018/2019 as part of a project<sup>2</sup> funded by the German Federal Ministry of Education and Research.

The short papers No. 4 and No. 18 by the Conference of the Independent German Federal and State Data Protection Supervisory Authorities (Data Protection Conference),<sup>3</sup> the DPIA simulation of the data protection authorities of Schleswig-Holstein, Mecklenburg-Western Pomerania and Lower Saxony<sup>4</sup> and the Standard Data Protection Model<sup>5</sup> recommended by the Data Protection Conference provided important orientation points for the approach, as did the German and English versions of the General Data Protection Regulation (GDPR)<sup>6</sup> and relevant commentaries.

Finally, we would like to express our sincere thanks to the project's advisory council and all the interview partners involved for their willingness to take part in the aforementioned workshops and interviews.

Karlsruhe, February 2020

## SUMMARY

# DATA PROTECTION IMPACT ASSESSMENT

This summary provides a heavily condensed overview of a possible procedure for a Data Protection Impact Assessment (DPIA) according to Article 35 GDPR.

## DPIA PROCEDURE

Overall, the data protection impact assessment (DPIA) to be conducted should be divided into five phases:

- I Initiation**
- II DPIA Preparation**
- III DPIA Execution**
- IV DPIA Implementation**
- V Sustainability**

**It is useful to divide these individual phases as follows:**

- Objective
- Input
- Roles and responsibility
- Implementation
- Output and results

In addition, certain documents should be provided in each phase. In the following, these are referred to:

- As the input or output of a phase and numbered consecutively **N**.

All the documents mentioned are listed at the end of the summary. The phases, their structure and the respective documents required in each case as well as the results to be documented are described in more detail for each phase below. Reference is made to the legal framework conditions of the GDPR that serve as a basis for the approach, in order to allow interested parties to obtain a more detailed treatment of the respective topic. This structure is a deliberately abstract representation of the procedure for conducting a DPIA and background knowledge of DPIA is therefore assumed. Chapters 4 to 8 in this handbook give more detailed information on the individual steps. Experience shows that conducting a DPIA also requires at least a basic knowledge of general data protection and data security issues (depending on the composition of the DPIA team).

## Initiation phase

### Objective:

Threshold assessment: clarify whether a DPIA is necessary (Article 35(1) GDPR).

### Input:

**1** Documentation of the new, envisaged or modified *processing operations* (with the information to be included in the records of processing activities according to Article 30(1) GDPR), *documentation concerning the lawfulness of processing* (according to Article 6 GDPR) and documented *preliminary considerations concerning the necessity and proportionality* of processing (complying with the principles of data protection, Article 5 GDPR)

### Roles / responsibility:

The *controller* of the processing activities (according to Article 4(7) GDPR) is responsible. Where necessary the controller is assisted by the *processor* (cf. Article 28(3)(f) GDPR), and accompanied during execution in an advisory capacity by the *data protection officer* (Article 35(2) GDPR).

### Implementation:

Clarify whether processing is likely to result in a high risk to the rights and freedoms of natural persons (cf. Article 35(1) GDPR). This includes examining the cases mentioned in Article 35(3) GDPR, checking the lists compiled by the supervisory authorities (cf. Article 35(4) and Article 68 GDPR), the criteria of the Article 29 Data Protection Working Party, and where appropriate, conducting an independent assessment of the existence and extent of risks to rights and freedoms in view of the nature, scope, context and purposes of the processing.

### Output:

**2** Documentation of the threshold assessment

### Result:

*If, as part of the threshold assessment, it is concluded that a processing operation is likely to result in a high risk to the rights and freedoms of natural persons according to Article 35(1) GDPR, a DPIA must be conducted.*



## DPIA preparation phase

### Objective:

A systematic description of the envisaged processing operations (Article 35(7)(a) GDPR) and of the concrete context from a technical, legal and organizational perspective; planning the execution of the DPIA.

### Input:

**1** *Documentation* of the new, envisaged or modified *processing operations* (with the information to be included in the records of processing activities in line with Article 30(1) GDPR), *documentation ensuring the lawfulness of processing* (in the sense of Article 6 GDPR) and *documented preliminary considerations concerning the necessity and proportionality* of the processing (considering the data protection principles in Article 5 GDPR)

**2** Documentation of the “positive” threshold assessment from Phase I

### Roles / responsibilities:

The *controller* (cf. Article 4(7) GDPR) of the processing shall carry out the DPIA prior to the processing (Article 35(1) GDPR), where applicable assisted by the *processor* (see Article 28(3) (f) GDPR). Implementation can be delegated to *persons with suitable competences*. The *data protection officer* accompanies the execution in an advisory capacity (Article 35(2) GDPR).

### Implementation:

a) Summary collection of information (Article 35(7)(a) GDPR):

- Data subjects, processed personal data, data flows, other stakeholders, (envisaged) processes
- Documentation of the (envisaged) technical implementation, technical infrastructure, already existing technical and organizational measures
- Where necessary, representatives of data subjects (e. g. works council, staff council, patient council), organization, processor, joint controller (jointly responsible for the processing), contracts etc

b) Proposal of a DPIA team for the execution phase and planning workshops/deadlines

### Output:

**3** Summary collection of information about the processing to be reviewed

**4** Proposed DPIA team for the execution phase and planning of workshops/deadlines

### Result:

Completion of the preparation phase to carry out the DPIA (Phase III).

## DPIA execution phase

### Objectives:

*Assessment of the risks of the envisaged processing to the rights and freedoms of (natural) persons (Article 35(7)(c) GDPR).*

*Selection of mitigation measures (safeguards) to address the risks and ensure the protection of personal data (Article 35(7)(d) GDPR).*

*Assessment of the necessity and proportionality of the envisaged processing operations in relation to the purposes (Article 35(7)(b) GDPR).*

### Input:

- 1** Documentation of the new, envisaged or modified *processing operations* (with the information to be included in the records of processing activities in line with Article 30(1) GDPR), *documentation ensuring the lawfulness of processing* (according to Article 6 GDPR) and documented *preliminary considerations concerning the necessity and proportionality* of the processing (considering the data protection principles in Article 5 GDPR)
- 2** Documentation of the “positive” threshold assessment from Phase I
- 3** Summary collection of information on the processing from Phase II
- 4** Proposed DPIA team for the execution phase and planning of workshops/deadlines from Phase II

### Roles / responsibilities:

The *controller* in the sense of Article 4(7) GDPR is responsible for carrying out the DPIA. Its implementation can be delegated to persons with suitable competences, referred to here as the DPIA team. Usually, the *DPIA team* will only partly comprise of persons with extensive knowledge of data protection, because other skills are required for the DPIA in addition to expertise in data protection. The *data protection officer* accompanies the execution of the DPIA in an advisory capacity (Article 35(2) GDPR). *Processors* can be consulted for assistance (cp. Article 28(3)(f) GDPR).

### Implementation:

- a) Identification and analysis of damage scenarios, in order to assess the risks to the rights and freedoms of natural persons. The following information is required for each damage scenario:
  - o Description of the scenario
  - o Data subjects
  - o Personal data

- o Stakeholders
  - o Potential damage to data subjects
  - o Elements triggering the occurrence of the damage
- b) Already existing technical and organizational measures (to be collected in parallel)
- c) Affected data protection goals and, where necessary, prioritization of the goals (consider which goals are particularly relevant or less relevant in the context of the analyzed scenario for the different data subjects)
- d) Assessment of the severity and likelihood of potential damage, derived from this: an assessment of the risk to rights and freedoms (Article 35(7)(c) GDPR)

#### **Interim result:**

Risk assessment, e. g. illustrated using a risk matrix (with the following key information: severity of potential damage/likelihood, see e).

- e) Selection of new, additional technical and organizational mitigation measures (safeguards), adjustment and further development of existing measures or modification of the processing (referred to in this document collectively as mitigation measures) in order to mitigate sufficiently the risks to the rights and freedoms of natural persons and to ensure the protection of personal data (Article 35(7)(d) GDPR)
- f) Assessment of remaining risks
- g) Assessment of the necessity and proportionality of the processing operations in relation to the purposes (Article 35(7)(b) GDPR)

#### **Output:**

**5** DPIA report (Article 35(7) GDPR)

#### **Result:**

*Answer to the question: Can the documented high risks be sufficiently mitigated using suitable technical and organizational measures?*

**Yes:** *Processing can be performed, subject to the successful implementation of the mitigation measures.*

**No:** *Consultation with supervisory authorities (Article 36(1) GDPR) by the controller or abandonment of the processing.*

## DPIA implementation phase

### Objective:

**Implementation of the mitigation measures (safeguards) defined in Phase III and documented in the DPIA report; on this basis, proof of compliance with the GDPR and approval of the processing, which can now go ahead.**

### Input:

- 5 DPIA report (Article 35(7) GDPR) from Phase III

### Roles / responsibilities:

The *controller* (in the sense of Article 4(7) GDPR) is responsible also for the implementation (Article 35 GDPR). The *DPIA team* provides support. The concrete implementation of suitable technical and organizational measures can be delegated to persons with suitable competences. The *data protection officer* accompanies the DPIA in an advisory capacity (Article 35(2) GDPR); performing the DPIA is monitored (Article 39(1)(c) GDPR).

### Implementation:

- a) Planning and implementation of the defined mitigation measures
- b) Planning and implementation of a test methodology, in order to test the effectiveness of the mitigation measures and monitor risks; the test results should be recorded
- c) Execution of the defined tests and documentation of the test results to the extent possible before approval of the processing
- d) If additional risks are identified during this process, these must also be addressed

### Output:

- 5 DPIA report
- 6 Documentation of the mitigation measures, the test methodology, and test records of the effectiveness of the mitigation measures and of monitoring the risks
- 7 Proof of compliance with the GDPR and approval of the processing, which can now go ahead

### Result:

*Proof of compliance with the GDPR and approval of the envisaged processing, which can now go ahead.*

After completing a DPIA, suitable measures must be taken to ensure its sustainability. In particular, these include monitoring the risks and regular reviews and adjustment of the DPIA in the light of changes in the context relevant to the risks associated with the processing operation (Article 5(2), Article 35(11), Article 39(1)(b) GDPR).

### Objective:

*Ongoing process ensuring that the risks to the rights and freedoms of natural persons are sufficiently mitigated and compliance with the GDPR is ensured.*

### Input:

5 DPIA report

6 Documentation of the mitigation measures, the test methodology and test records of the effectiveness of the mitigation measures and monitoring the risks from Phase IV

### Roles / responsibilities:

The controller must carry out the review (Article 35(11) GDPR), the data protection officer must monitor compliance with the GDPR (Article 39(1)(b) GDPR), where applicable, further responsibilities for monitoring according to national regulations (for example, in Germany, the works council in accordance with the Works Constitution Act (BVerfG)).

### Implementation:

The measures to ensure sustainability should be incorporated into a data protection management system, if possible:

- a) Review the effectiveness of mitigation measures, monitor the risks based on a test methodology, and document the execution of the test according to the methodology
- b) Identify deviations in relation to the effectiveness of mitigation measures and the risks
- c) Document the results of the review

In the case of smaller deviations in relation to the effectiveness of mitigation measures or changes regarding the processing:

- d) Adjust the risk assessment, the mitigation measures, and the related test methodology
- e) Adjust the DPIA report

In the case of larger deviations in relation to the effectiveness of the mitigation measures or major changes regarding the processing:

- f) Repeat Phases II to IV of the DPIA

### Output:

- 5 DPIA report (modified if necessary)
- 6 Documentation of the mitigation measures, test methodology and test records on the effectiveness of mitigation measures and monitoring the risks (adjusted if necessary)

### Result:

*The processing operation reviewed by the DPIA continues to meet the necessary requirements so that the processing does not result in a high risk to the rights and freedoms of the data subjects.*

## Overview of documents in the context of the DPIA

- 1 Documentation of the new, envisaged or modified processing operations (with the information to be included in the records of processing activities in line with Article 30(1) GDPR), documentation ensuring the lawfulness of processing (in the sense of Article 6 GDPR) and documented preliminary considerations concerning the necessity and proportionality of the processing (considering the data protection principles in Article 5 GDPR)
- 2 Documentation of the “positive” threshold assessment
- 3 Summary collection of information concerning the nature, scope, context and purposes of the processing and all other information relevant for the review
- 4 Proposal of the DPIA team to carry out the execution phase and planning workshops/deadlines
- 5 DPIA report
- 6 Documentation of the mitigation measures, test methodology and test records of the effectiveness of mitigation measures and of monitoring the risks.
- 7 Proof of compliance with the GDPR and approval of the processing, which can now go ahead

## 1 Introduction

According to Article 35 of the General Data Protection Regulation (GDPR), under certain conditions, the controller – according to Article 4(7) GDPR – shall carry out a “data protection impact assessment” (DPIA). The purpose of the DPIA is to identify, assess and mitigate any risks to the rights and freedoms of affected (natural) persons that may result from data processing. Although the General Data Protection Regulation defines minimum requirements that a data protection impact assessment must fulfill, it does not stipulate a process with criteria that must be followed.

Different methods for carrying out a DPIA have therefore been published since 2018. This handbook operationalizes one of these methods for practical application in companies and public authorities. The method described here was developed by the research consortium *Forum Privacy and Self-Determination in a Digital World* funded by the German Federal Ministry of Education and Research, and, in a subsequent research project, was then tested in twelve interviews and workshops with companies and public authorities and further developed on this basis for practical application.

### 1.1 Data protection

The term “data protection” is frequently misunderstood. Contrary to its wording, it does not concern the protection of data (the field of data security), but the protection of the natural persons to whom the information refers (data protection). In other words, data protection should protect the freedom of individuals to decide themselves how their data are handled and who may obtain what information (right to informational self-determination), although this is not an unlimited right. Indeed, there are conceivable circumstances in which persons must pass on their data, for example, to receive benefits, interact with others or be able to engage in legal transactions. However, precisely then it is important that the respective individual is protected from the organization conducting the processing (i.e. the companies involved, public authorities such as state institutions, the police, or schools, but also clubs and associations, churches, or non-governmental organizations). This is important because there is often an imbalance of power between the individual, whose data is processed, and the bodies (organizations) conducting the processing, which

are usually privy to extensive information about persons (e. g. about their employees, beneficiaries, wards, users, customers etc.). These data can be used in principle for all sorts of purposes, often with damaging consequences for the data subjects. In addition to material and physical damages, e. g. job loss, discrimination or violent crime, non-material damages are also conceivable, such as loss of reputation or the vague feeling of being “spied on”. In this context, it is worth mentioning the danger of so-called chilling effects, when persons fall into a kind of self-censorship (due to concerns about the possible accumulation of information about them) and preemptively limit their expressions and actions themselves.

Among other things, data protection law helps to mitigate this imbalance of power between organizations and individuals, not least to protect individual autonomy. One step towards this is that the processing of personal data requires compliance with certain principles – summarized in the data protection principles of Article 5(1) GDPR. Another step is that data subjects are accorded certain rights, for example, access, information, rectification, objection, erasure, and data portability (see Articles 12–22 GDPR). Together with the other rights and obligations of data protection, these serve to guarantee that persons whose data are processed or to whom the data directly or indirectly refer to (data subjects), have a degree of control over the processing of their personal data that ensures protection against damages and safeguards their autonomy.

The subject of data protection is therefore the person who is identifiable using the processed data (the data subject). Correspondingly, only those data that allow conclusions to be drawn about natural persons – i.e. relate to an identified or identifiable person – are subject to data protection law. In other words, information that can be used to identify persons (cp. Article 4(1) GDPR). Data that cannot be traced back to identifiable persons (e. g. data about natural phenomena) are not subject to data protection (although there may be data security requirements). However, due to the growing possibilities to link and evaluate data, it should be noted that even data that do not, at first glance, seem to relate to a person can be combined with additional data to identify persons (often discussed under headings such as *Artificial Intelligence* and *Big Data*).

In addition to external attackers, the organization itself is a significant source of risk in data protection. Data protection is therefore also about protecting data subjects against processing operations that the organization carries out in a manner that is formally correct according to its *own, internal* rules and processes and that are suitable for its purposes (profit, administrative efficiency etc.), but that are illegitimate in terms of (data protection) law.

In this sense, data protection goes beyond IT security and is clearly different from it. In contrast to IT security, risk sources are not just technical failures or malfunctions or the actions of unauthorized insiders and outsiders (“hackers”), but especially the



regular, planned activities of the organization itself. Whereas IT security treats the organization as the thing to protect, in data protection, it is the data subjects that need protecting – and the organization itself with all its entities (departments, employees, suppliers) is often considered one of the main “attackers”.

## 1.2 Data protection impact assessment

The data protection impact assessment (DPIA), according to Article 35 GDPR, is an instrument to identify, assess and mitigate risks to the rights and freedoms of a natural person that may arise from a data processing operation. Unlike the technical and organizational measures that must always be implemented for processing activities in accordance with Article 32 GDPR, a DPIA must only be carried out, according to Article 35(1) GDPR, if an envisaged processing is likely to result in a “high risk” to the rights and freedoms of natural persons. How such a “high risk” to the rights and freedoms of a natural person can be determined in order to decide whether to carry out a DPIA is explained in more detail in Chapter 4.

If this condition is met, the GDPR only requires that a DPIA is conducted, without extensively specifying the method to be used. However, four minimum requirements are set that a DPIA must meet.

According to Article 35(7) GDPR, a DPIA must contain the following:

- a) a systematic description of the envisaged processing operations and the purposes of the processing including, where applicable, the legitimate interest pursued by the controller;
- b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- c) an assessment of the risks to the rights and freedoms of the data subjects [...];
- d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation [GDPR], taking into account the rights and legitimate interests of data subjects and other persons concerned.

In addition, as part of the DPIA, Article 35(9) GDPR includes a reference that controllers shall seek the views of data subjects or their representatives where appropriate, although the formulation does not contain a concrete obligation to do so. Nevertheless, consulting, or at least involving, the data subjects or their representatives often seems useful. It can serve as a basis for determining whether other views exist that are relevant to the DPIA and, as a result, help the supervisory authorities if they have to conduct audits to determine whether a DPIA has been carried out appropriately and in the necessary depth.

After completing these steps and implementing the technical and organizational measures needed to mitigate the risks, the envisaged processing can be approved and go ahead – provided the risks were sufficiently mitigated. If the risks could not be sufficiently mitigated, the processing may not be carried out. In this case, the controller must abandon the envisaged processing or consult the supervisory authorities in line with Article 36 GDPR.

If, following approval, the processing is carried out, Article 35(11) GDPR requires the controller to review subsequently, where necessary, whether the processing is actually performed in accordance with the requirements of the mitigation measures determined by the DPIA, i.e. whether all the risks are still sufficiently mitigated. Such a review must be carried out according to Article 35(11) GDPR at least “when there is a change of the risk represented by processing operations”.

Article 35(11) GDPR therefore implies that the controller should view the DPIA as a “living” document, which evolves during the life cycle of the processing operation, and for which an adequate monitoring system is established by the controller, preferably as part of a data protection management system, to identify possible changes of the risks and to review the effectiveness of the mitigation measures. The DPIA is to be documented and presented to the supervisory authorities on request, but does not have to be published.

## 1.3 Responsibility for the DPIA

Article 35 GDPR assigns the obligation to carry out a data protection impact assessment to the controller. However, the GDPR does not ignore the fact that other groups can also have important functions for the assessments done within the scope of a DPIA. At different points, it mentions (possible) processors and data protection officers as well as others with different functions within the scope of a DPIA. The data subjects or their representatives should also be included in a DPIA where applicable.

### Controller

According to the wording of Article 35(1) GDPR, the controller is legally obliged to carry out a DPIA. Controller, as defined by the GDPR in Article 4(7), can be a natural or legal person, public authority, agency, or other body independently of whether this is a public body or not. The responsibility to comply with the legal requirements of data protection is therefore delegated to the legal entity processing the data, represented by its management, i.e. ultimately the management level of a company, authority, agency or other body (hereafter organization).<sup>7</sup> In order to be a controller, according to Article 4(7) GDPR, an entity must determine, alone or jointly with others, the purposes and means of the processing; this distinguishes them from processors and other stakeholders.

Accordingly, neither the processor nor other stakeholders (e. g. manufacturers of individual components used for the processing operation, e. g. hardware or software) are covered by the obligation to carry out a DPIA.

However, when carrying out a DPIA, controllers are free to delegate the operational execution and implementation of the DPIA either to employees with relevant expertise, such as those closely involved with the processing operation in question, or to external third parties (consultants).

### Data protection officer

The data protection officer (DPO) has a special role in the DPIA. At least in Germany, if controllers undertake processing operations that necessitate a DPIA, they are also obligated to appoint a DPO as per §38(1) BDSGC. Article 35(2) GDPR and Article 39(1)(c) GDPR provide that the controller shall seek the advice of a data protection officer for a DPIA, who monitors its performance. Although the GDPR does not explicitly forbid that performance of the DPIA be delegated to the DPO, this type of delegation does not seem compatible with the officer's legally mandated monitoring task, since it is hard to imagine that the law would encourage such a dual role.<sup>8</sup> The background to this is that, on the one hand, the advice of a data protection officer should be consulted when performing a DPIA, which implies that the DPO is advising a third party separate from herself. After all, it would be redundant for the DPO to advise herself. On the other hand, the DPO has the task of independently monitoring the performance of a DPIA, again implying that another party is being monitored, since it would be equally redundant for the DPO to monitor herself. Therefore it is to be expected that the supervisory authorities will oppose any delegation of the task of carrying out the DPIA to the DPO. Accordingly, the admissibility of any DPIA that was performed under such circumstances (i.e., by the DPO in some sort of a "dual" role) must be in doubt.

However, due to this legally mandated advisory task, the data protection officer can still play an extensive role in the DPIA. For instance, the Article 29 Data Protection Working Party advises controllers to seek the advice of the DPO on all major questions surrounding a DPIA. In particular, advice should be sought on the following issues:

- whether to perform a DPIA
- what method should be used to perform the DPIA
- whether the DPIA is to be performed within the organization or by an external service provider
- what protective measures should be used to mitigate the risks to the data subjects
- whether the DPIA has been carried out correctly and the decisions made on its basis (whether to perform the envisaged processing, selection and implementation of protective measures) are in compliance with the GDPR<sup>9</sup>

It is up to the controller whether or not to follow the advice of the data protection officer, but such a decision and its reasons must be documented in writing in the DPIA documentation. The controller always has the final authority to make a decision about the DPIA and all its related issues and this may not be delegated to the DPO. The controller is also always liable for the correct application of the GDPR including the DPIA in accordance with Article 24(1) GDPR.

### Product producers, processors, and joint controllers

**Product producers**, who do not process data themselves but only supply the systems and components used to perform processing, are not obliged, under Article 35 GDPR, to carry out a DPIA for their products. However, it is frequently the producers themselves who have the best understanding of the technical characteristics of their products that are relevant for security and data protection issues. It seems sensible, if only for reasons of economic self-interest, for them to provide the best possible documentation, so that potential customers can integrate these descriptions as easily as possible within a DPIA when using the components for the relevant processing operation. In addition, there is the possibility in individual cases that a high risk under Article 35(1) GDPR may be triggered when producing single components of a processing system (e. g. hardware or software) in combination with other factors. In individual cases, it can therefore make sense – and be of advantage to producers – to think about data protection-friendly settings and advice for potential customers at an early stage, within the scope of data protection by design and by default, in order to mitigate possible risks in advance, or at least to be able to show alternatives.

**Processors** are natural or legal persons who process personal data on behalf of a controller, but who have no decision-making power over the purposes and means of the processing operation (cf. Article 4(7) and (8) GDPR). In accordance with Article 28(3)(f) GDPR, they are obliged to assist the controller in ensuring compliance with the DPIA. In specific cases, this is likely to concern providing the controller with the necessary information.

**Joint controllers** are present according to Article 26(1) GDPR, whenever two or more controllers jointly determine the purposes and means of processing. In this case, the Article 29 Data Protection Working Party requires the controllers to determine their respective responsibilities and to indicate in the DPIA which controller is responsible for which mitigation measure. In addition, they must assist each other in conducting the DPIA and in providing “useful information” for the process.<sup>10</sup>

### **Practical tip** IT service providers

Especially for IT service providers who supply individual software or hardware components and are responsible for some parts of data processing operations, it can be difficult to decide in an individual case whether this amounts to commissioned data processing or joint control. In any case, the requirement for service providers to actively participate in the DPIA and assume responsibility for identifying and analysing risks and implementing mitigation measures is likely to increase in relation to the degree to which they can themselves take decisions about the means and purposes of the processing operation. This is particularly true the greater the potential for negative impacts on the data subjects from activities undertaken by the service providers are. Conversely, it may be not only practically possible for such service providers to produce “generic” elements of a DPIA for typical applications in which their services are used (e.g. communication services in the health-care sector), but also economically beneficial, and to provide already reviewed processing operations as documentation as well as to develop options for technical and organizational measures that facilitate data protection by design and by default. Customers (controllers) can then use the generic DPIA to compile a DPIA for the processing operation in their specific context or to take relevant mitigation measures to address risks.

.....  
A practical approach to DPIA  
.....

## 2 Necessary preliminary work

Certain information must be available in advance in order to carry out a DPIA. This refers to the records of processing activities (hereafter “processing records”), a documentation of the legal basis for the processing and an assessment of the necessity of the envisaged processing related to its purpose. If these are missing, it is very difficult to carry out a DPIA due to the complexity of the processes considered.

Making a preliminary assessment of the proportionality of the envisaged processing before beginning the DPIA is not required but nevertheless useful. This assessment is explicitly provisional and not yet complete and is done in order to be able to react to any existing proportionality deficit at an early stage.

### 2.1 Records of processing activities according to Article 30 GDPR

In accordance with Article 30(1) GDPR, controllers must maintain a record of all the processing activities under their responsibility. These records must contain certain information. Although certain small enterprises are exempted from the obligation under Article 30(5) GDPR, processing records must be maintained as soon as the processing performed engenders risks to the rights and freedoms of the data subjects, or concerns special categories of personal data referred to in Article 9(1) GDPR. It would be almost impossible to carry out a DPIA without this basic information and it should therefore already be available when starting the DPIA.

The information to be provided in the records of processing activities according to Article 30(1) GDPR:

- name and contact details of the controller, representative and data protection officer (where applicable)
- purposes of the processing
- description of the categories of data subjects affected by the processing
- description of the categories of the processed personal data
- categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organizations
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards
- the envisaged time limits for erasure of the different categories of data (where possible)
- general description of the technical and organizational security measures referred to in Article 32(1) GDPR (where possible)

If processing records have not yet been compiled – for example, because the processing is still in the planning stage – the information mentioned should be collected in advance as far as possible.

## 2.2 Stakeholders

Often, several stakeholders within or outside an enterprise, state institution or other organization are involved in a processing operation this organization is responsible for (departments within the organization, processor outside the organization, possible joint controllers, etc.), e. g. because they carry out parts of the processing, are given access to data or supply data, or administer the relevant IT systems and services. As any of these stakeholders could in principle constitute sources of risks to the data subjects, their representatives should be integrated into the DPIA process where possible. Consequently, it is necessary to identify all stakeholders in advance.

## 2.3 Documentation of the legal basis of processing

According to Article 5(1)(a) GDPR, any processing of personal data requires a legal basis. Any processing conducted without an effective legal basis constitutes an infringement of the fundamental right to data protection according to Article 8 CFREU, and thus, the occurrence of a risk to the rights and freedoms of the data subjects as well as an infringement of the GDPR. In order to avoid this, the legal basis for the envisaged processing should be documented in advance.

Article 6(1)(a)–(f) GDPR lists six possible legal grounds for processing personal data. If special categories of personal data are processed as referred to in Article 9(1) GDPR, or personal data relating to criminal convictions and offences in accordance with Article 10 GDPR, the supplemental legal grounds relevant for these types of personal data must also be considered during the processing.

If several separate legal entities are involved in one processing operation, which in addition also process different personal data of different data subjects, these different processing operations may have to be based on separate legal grounds. It should be ensured that each specific processing operation, and therefore the processing as a whole, is covered by a legal basis. In such cases, it is advisable to draw a diagram showing the stakeholders, data subjects, processing operations and legal relationships (including existing data flows).

## 2.4 Assessing the necessity and proportionality of processing

According to Article 35(7)(b) GDPR, part of the DPIA must contain an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

The principle of data minimization (Article 5(1)(c) GDPR) operationalizes the question of **necessity**. This concerns assessing whether the processing operations, including the data collected for them, are all really necessary to fulfill the purposes of the processing, or whether the purposes could be achieved by alternative ways that are less intrusive on the rights and freedoms of the data subjects. It makes sense to conduct this assessment in advance: first, because any processing of personal data – even those that do not trigger the obligation to conduct a DPIA – must comply with the principle of data minimization; second, because any necessary adjustments to the processing operations can be made in good time.

The **proportionality** of a data processing is only given if the disadvantages of the processing for the data subjects – including the infringement on their fundamental right to data protection in accordance with Article 8 CFREU that occurs with each processing of personal data as well as possible infringements on other rights – are in an appropriate balance to the advantages of the processing for the legitimate interests of the controller. It is difficult to set a general rule for assessing proportionality, because the rights and interests that must be weighed up against each other are likely to differ from case to case. In order to arrive at a final conclusion about the proportionality of the processing, the assessment of the risks must be available (described in Chapter 6) that occur for the data subjects due to the processing. Ultimately, it is only possible to judge whether the advantages for the controller are in an appropriate balance to the disadvantages (i.e. risks) for the data subjects if it has been clarified what risks exist and how severe these are.

### Practical tip Preliminary assessment of proportionality

It is advisable nevertheless to perform a provisional “preliminary assessment” of proportionality at the outset, in addition to the assessment of necessity, and to ask whether the infringement on the rights and freedoms of data subjects represented by the envisaged processing are proportionate. If the rights and interests of the data subjects obviously outweigh the interests of the controllers – based on clear case law or generally acceptable social norms – then the processing should cease immediately or be modified so that it no longer violates the relevant case law or norms.

This preliminary assessment cannot fulfill the requirement of Article 35(7)(b) GDPR. As described above, a complete assessment of proportionality is only possible based on the risk assessment to be carried out within the DPIA. Rather, this preliminary assessment serves the general purpose of forward-looking and ethical technology design.



### 3 DPIA phases

Carrying out a DPIA should follow as structured an approach as possible, to make it easy to (subsequently) still follow and comprehend the documentation produced during the DPIA. It is therefore advisable to write up at least brief minutes for each task in the DPIA, and also note down the names of the persons present for future reference.

Due to the sheer scale of a DPIA, it is helpful to divide it into different phases. A subdivision into five phases has proven useful:

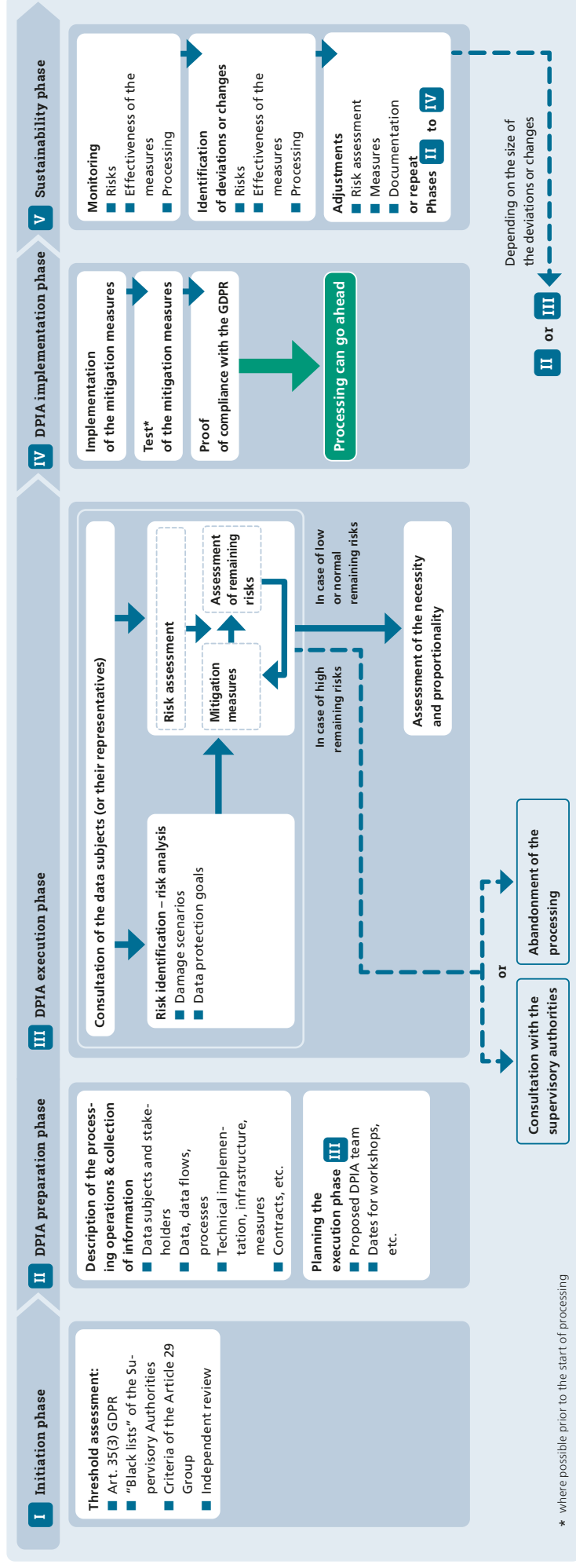
**I Initiation phase**, also referred to as a threshold assessment, which ascertains whether a DPIA is necessary

**II Preparation phase**, in which the documents and information needed for the processing, relevant data flows and technical systems, data subjects and legal basis are collected, so that a systematic description of the envisaged processing operations can be drawn up, the DPIA team is assembled and the DPIA planned

**III Execution phase**, in which the information collected in Phase II is validated, risks are identified, analyzed, and assessed (referred to hereafter collectively as risk assessment), suitable mitigation measures are selected and the necessity and proportionality of the processing are assessed

**IV Implementation phase**, in which the mitigation measures selected in Phase III are implemented, evidence is provided of compliance with the GDPR and the processing can be approved and go ahead

**V Sustainability phase**, in which a continuous review and adaptation of the processing operation takes place throughout its life cycle in order to prove that the risks to the data subjects resulting from the processing operation are sufficiently mitigated



**Figure 1:**

The sequence of the five phases of a DPIA

### 4.1 Approach

According to Article 35(1) GDPR, a DPIA must be carried out if a type of processing “is likely to result in a high risk to the rights and freedoms of natural persons”. In order to ascertain whether such a high risk is likely to exist, the following three sources of information should be used:

- The requirements of Article 35(3) GDPR
- Lists of the supervisory authority
- Criteria of the Article 29 Data Protection Working Party

An additional independent assessment of the likely extent and existence of risks to the rights and freedoms of natural persons is indispensable.

These assessments can be made by the controller or by a third party appointed by the controller, where necessary, assisted by the processor and the specialist departments responsible for the processing. The data protection officer should be involved in an advisory capacity.

When planning and developing new processing operations, it is advisable to assess whether a DPIA is necessary at an early stage, because the scope for design changes is usually still relatively large then and changes are simple and cost-effective. A DPIA accompanying this process can also ensure implementation of the principle of data protection by design and by default.

Essential inputs to the threshold assessment are, first, comprehensive documentation of the processing activities to be assessed (in addition to the information needed for the processing records) and, second, documentation of the legal basis of the processing.

A draft version of these documents may suffice – for instance if the processing is still in such an early stage of planning that a final version is not yet available. However, if changes are made to the envisaged processing or its legal basis at a later stage, it will be necessary to review whether these changes affect the results of the threshold assessment and the DPIA that may have already been carried out. If this is the case, both must be conducted again or modified.

The next sections describe the information sources.

## 4.2 Reviewing the requirements of Article 35(3) GDPR

Article 35(3)(a)–(c) GDPR cites three cases, which make a DPIA necessary:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (Article 35(3)(a)).
- processing on a large scale of special categories of data referred to in Article 9(1) GDPR or of personal data relating to criminal convictions and offences referred to in Article 10 GDPR (Article 35(3)(b));
- a systematic monitoring of a publicly accessible area on a large scale (Article 35(3)(c)).

A clarification of the concept of “on a large scale” can be found in the guidelines of the Article 29 Data Protection Working Party (see below).

### Data processed “on a large scale”

The Article 29 Data Protection Working Party refrains from defining a generally applicable quantitative threshold that constitutes processing “on a large scale”; instead it outlines four criteria and several examples that can be used as a basis to determine whether the processing can be classified as “large scale”. These criteria are:

- the number of data subjects considered, either as a specific number or as a proportion of the relevant population
- the volume of data and/or the range of different data items being processed
- the duration or permanence of the data processing activity
- the geographical extent of the processing activity

Examples of processing “on a large scale” as defined by the Article 29 Data Protection Working Party are:

- a hospital processing patients’ data as part of its normal routines
- processing the travel data of natural persons in the local public transport system (e. g. tracking them using travel cards)
- processing the real-time geolocation data of the customers of an international fast food chain for statistical purposes by a specialized processor
- processing customer data in a bank or insurance company as part of its normal business operations
- processing of personal data by a search engine for the purposes of behavioral advertising
- processing of data (contents, volume of data traffic, location) by telephone and internet providers.

Examples of data processing operations that are not “on a large scale” include:

- Processing patient data by an individual doctor
- Processing personal data relating to criminal convictions and offences by individual lawyers

Source: Article 29 Data Protection Working Party, “Guidelines on Data Protection Officers”, p. 8–9

## 4.3 Lists of the data protection supervisory authorities

According to Article 35(4) GDPR, the supervisory authorities are obliged to publish a list of the kind of processing operations for which a DPIA is required. These lists are referred to as “positive lists” or blacklists. If the envisaged processing appears on a blacklist, conducting a DPIA is mandatory.

The Conference of the Independent German Federal and State Data Protection Supervisory Authorities (Data Protection Conference) has published a blacklist for the private sector of 17 processing operations with examples and typical applications for which a DPIA must always be conducted.<sup>11</sup> This list is definitive for the private sector in Germany. For the public sector, the individual data protection supervisory authorities of the federal and state governments have also published relevant lists corresponding to the respective federal/state data protection laws.

The lists are subject to the consistency mechanism of the European Data Protection Board. The Board issues an opinion on these lists and recommends adaptations where necessary. The aim is not to compile a uniform, EU-wide list, but rather to avoid “significant inconsistencies”. The supervisory authorities have “a margin of discretion with regard to the national or regional context”.<sup>12</sup> The lists of the respective Member States should therefore be consulted for processing that takes place across national borders.

When working with the lists, it is important to remember that these – as also emphasized by the supervisory authorities – are non-exhaustive. If an envisaged processing does not appear on the list, this by no means indicates that the existence of a high risk can be excluded and a DPIA is not required. On the contrary, in this case, the threshold assessment should be continued by examining the criteria of the Article 29 Data Protection Working Party.

## 4.4 Criteria of Article 29 Data Protection Working Party

The Article 29 Data Protection Working Party has compiled 9 criteria that can indicate a high risk.<sup>13</sup>

According to Article 29 Data Protection Working Party, a “high risk” is assumed to be likely, and a DPIA must be conducted, if the envisaged processing operation meets two of these criteria. However, a high risk can still be present (and a DPIA mandatory) if only one – or indeed none – of the criteria applies.

If only one criterion applies, an independent assessment must be conducted of whether the processing is likely to result in high risks to the rights and freedoms of data subjects. If it is likely, a DPIA must be conducted. If the decision is made that, despite meeting one criterion, a high risk is not likely and a DPIA is not required, the reasons for this decision must be documented so that this can be presented to the supervisory authorities upon request.

Like the list, the criteria of the Article 29 Data Protection Working Party are non-exhaustive. An independent review should therefore always be conducted in addition.

## 4.5 Independent review

In addition to using the information sources described above, the controller should also generally assess whether the processing is likely to result in a high risk to the data subjects based on its nature, scope, context, and purposes. Especially new technological developments may not yet be included in the lists of the data protection supervisory authorities. The risk analysis described in chapter 6 can be used as an orientation for this assessment. The assessment does not need to replicate a full DPIA risk analysis – also in terms of time and effort. Instead, corresponding to the steps described in chapter 6, the aim is to consider what the envisaged processing actually does (for what purpose it collects and processes personal data and how), who the data subjects and stakeholders are, and whether plausible scenarios are conceivable, in which the processing could result in significant risks to data subjects. If it does, a DPIA must be initiated, otherwise a DPIA is not needed. However, since a DPIA is a good instrument to prevent possible risks and to ensure compliance with the GDPR, the controller is advised to carry out a DPIA in case of doubt.

## 4.6 Documentation of the result

A practical approach to DPIA

I

Although the GDPR does not stipulate that the results of the threshold assessment must be documented, this is always useful in terms of being able to verify compliance, so that it can be presented to the data protection authorities on request. The results and reasons for the decision should be documented. It would make sense to integrate this information into a data protection management system.

### 5.1 Approach

If the threshold assessment indicates that a DPIA must be carried out, a systematic description of the envisaged processing operations (Article 35(7)(a) GDPR) and the specific context must be made from a technical, legal, and organizational perspective. This is required for the risk assessment in the subsequent execution phase. The data subjects and the participants are identified in this context. In addition, the team executing the DPIA is brought together and the subsequent execution phase planned.

This information can be compiled either by the controller or a third party appointed by the controller, assisted where necessary by the processor and the specialist departments responsible for the processing. The data protection officer should be involved in an advisory capacity.

### 5.2 Collection of information and description of the processing operations and the purposes of the processing

Making a systematic description of the envisaged processing operations and the purposes of the processing fulfills the first of the four requirements for a DPIA cited in Articles 35(7)(a)–(d) GDPR, namely the preparation

*of a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller (Article 35(7)(a)).*

The purpose should already be provided in the processing records. It should be noted that additional purposes are sometimes “discovered” while carrying out the DPIA that were not documented in the description of the processing operation, but that are also served by the processing in question. In this case, these must be added to the description of the purpose and the processing records. A review must also be conducted as to whether these “new” purposes are also covered by the corresponding legal bases.

In order to describe the processing operations, it usually makes sense to document the following information:

- data subjects, processed personal data, data flows, other stakeholders, (envisaged) processes
- documentation of the (envisaged) technical implementation, technical infrastructure, technical and organizational measures



- where necessary, data subject representatives (e. g. works council, staff council, patient council), organization, processor, joint controllers (jointly responsible for the processing), contracts etc

In order to clarify the processing operations and to identify the data subjects, categories of personal data and other stakeholders as comprehensively as possible, it is often helpful to produce a data flow diagram, which documents the entire processing operation from collection, storage, utilization, and transfer through to erasure. Documents should be compiled on the systems, networks, technical infrastructures and plans to implement the processing identified in this way. In particular, this should consider already planned technical and organizational measures. In the subsequent execution phase, the DPIA team should be in a position, based on this information, to define and analyze possible damages to data subjects in the context of the considered processing.

#### **Practical tip** Dealing with levels of granularity and complexity

One problem when describing the processing is to get the right level of granularity – neither too detailed, nor too superficial. It is difficult to set general rules here. One way of classifying which information should be recorded is to work backwards from the end result: ultimately, the description of the processing operations should enable a reliable identification, analysis and assessment of risks and selection of mitigation measures. The description can also be approached iteratively: to start with, it is often most important to obtain a reliable outline of the components of the processing and the stakeholders involved so that possible risks can be identified. Additional detailed information can be collected afterwards where necessary.

Another possible challenge is that, on closer examination, the subject matter can quickly become very complex because processing is performed using extensive technical infrastructures, is frequently networked with other systems and involves several locations and additional processors and their technical systems and processes if necessary.

Usually, there is no quick solution to this problem. If it can be assumed that the identified additional processing operations represent high risks to data subjects, a DPIA must be conducted for them as well. In such situations, it may be useful to start by separating the different processing operations as much as possible (both in view of their purposes and the used data, IT systems, and processing operations and stakeholders) and then to work through them successively using a DPIA. If the different processing operations are closely interrelated, it should be possible to reuse relatively large amounts of information and documentations in the different DPIAs. The focus should then be on where the individual processing operations actually have (risk-relevant) differences.

A related challenge arises if basically the same or similar processing operations are used in different contexts, for instance, because the same service is offered to several clients. As mentioned in Chapter 1.3.3, this can often involve joint control-ership. Since the context and details of the implementation are different for each customer, it must be assumed that the risks and any required mitigation measures will also vary from customer to customer. This is why it is likely that a separate DPIA must be produced for each customer. To keep the workload involved as low as possible, in this situation, it is advisable to produce one or several “generic” DPIAs for “typical” implementations and contexts of the service in question, and then to use these as templates for DPIAs for other implementations. This will involve documenting the relevant differences in the context and implementation as reliably as possible, so that customer-specific risks can be identified and mitigated in each case.

### 5.3 Identification of the data subjects

According to Article 4(1) GDPR, data subjects are all the natural persons who are or could be identified directly or indirectly using the processed data. Legal persons are not data subjects in this sense; they are not covered by the data protection law (see Recital 14 GDPR).

Due to the data analysis methods used today and the possibility to link data sets, it is likely that even data that are not directly related to a natural person can still be linked to a natural person. GPS data of vehicles, for instance, or log data of machines can often be linked to a specific person. Even if these data were recorded to manage a company’s vehicle fleet, or to monitor the capacity utilization of a machine and to obtain information about when maintenance is due, they are able to be related to a person, so that personal data in the sense of the GDPR are being processed.

To make a reliable identification of the data subjects, it can be helpful to answer three questions:

1. Whose data should the system collect?
2. Whose data are collected in addition to this, including indirectly or as “bycatch”?
3. Who else is it possible to identify based on the collected or processed data?

Typical categories of data subjects are:

- **Employees** of the organization and the **staff** of its customers, suppliers, or service providers
- **Customers** and **users** of digital services and digitalized formerly “analog” products (e. g. smart cars, smart TVs) as well as **their relatives, friends, and other persons**, who come “into contact” with these products (e. g. as passengers, or as persons present in a room with voice recognition devices)
- **Patients, care home residents, school children** and **recipients** of state benefits as well as their relatives, friends, and other persons
- **Policyholders** and **recipients of other financial services** and their relatives
- **Uninvolved citizens** and **passers-by** (e. g. in video surveillance)

**Practical tip** Always consider employees among the data subjects

Employees and individual staff members of third parties are frequently found among the data subjects – even if it is not the purpose of the processing to analyze their data. The reason is that most digital work appliances automatically record data that could be used to monitor and control employee performance. The risks that processing employee data could pose should therefore always be considered and the relevant protective measures should be taken where necessary.

## 5.4 Identification of other stakeholders

Stakeholders are all the organization – internal and external, natural and legal persons (businesses, state institutions, non-governmental organizations, external attackers, others) as well organizational units without independent legal status (e. g. other company departments) – that already have access to the data used in the processing, IT systems and processing operations, or could plausibly access them or potentially influence them.

The neutral term “stakeholder” was chosen deliberately. Being a stakeholder does not imply any kind of illegitimate behavior or “malicious intent”. All persons and institutions that enjoy completely legitimate access are also stakeholders. Nevertheless, stakeholders are often the most important source of risk for data subjects. Problematic activities of stakeholders need not necessarily be traced back to malicious intent, but may even have the opposite motivation (e. g. in the context of care) of wanting to help the data subjects. It is therefore important to identify – without judging – all the current or potential, direct and indirect, internal and external stakeholders.

The identification of stakeholders should include an analysis of their motives, interests, and abilities to obtain access to or to influence the data and processing operations.

This information is important for the identification and analysis of risks that takes place later. This should also consider possible motives of the stakeholders legitimately involved in the processing to go beyond the purpose of the processing.

Finally, it should be considered that access/influence can also occur without motive and even unintentionally. For example, employees can unintentionally obtain access to data because business partners send them data improperly and without it having been requested or announced. If such a scenario is conceivable, these employees should be considered as stakeholders – even if they have no desire to be!

To identify all the stakeholders, it may be helpful to answer the following questions:

1. Which internal and external stakeholders – including the processors – are actively involved in the processing operation?
2. Who else has access to the data and processing operations (without already being actively involved in the processing) or could otherwise influence or exploit the processing operation?
3. What interests do the stakeholders identified in steps 1 and 2 have that they could pursue by using the data or by influencing the processing operations in some other way, even beyond the defined purposes of the processing?
4. Which other internal or external stakeholders that are not yet actively involved in the processing could be interested in the data and/or processing operations and be motivated and able to obtain access or influence?
5. Who else might gain access or influence, possibly unintentionally, and if so how?

### Practical tip Typical stakeholders

#### Internal

- Employees (including former employees)
- Managers and supervisors
- “Data-intensive” departments like marketing, personnel/HR, product development, IT
- Visitors (business and private)

#### External

- Companies, e. g.:
  - Providers of IT services, systems, and infrastructures
  - Suppliers, service providers and customers of the organization in general
  - Banks, insurances
  - Advertisers
  - Credit rating agencies, address and data traders, market research
  - “Data-intensive” technology developers

- State agencies, e. g.:
  - Benefits administrators like job centers, social and youth welfare agencies, pension funds
  - Security agencies
  - Statistical departments
- Health care organizations, e. g.:
  - Hospitals and care homes
  - Health insurance companies
- Research
  - Universities and non-university research organizations
- (Cyber-)criminals/hackers

## 5.5 DPIA team

A DPIA is usually carried out by a team, because single individuals rarely possess all the relevant knowledge. The precise composition of the team will vary from organization to organization. It is usually advisable for the following expertise and departments to be represented:

- **Legal expertise**, especially in **data protection law**
- **Operational data protection** and the **data protection officer**
- **IT expertise**
- (relevant) **specialist departments** including their **workforce**
- (where applicable) **works council** and **representatives of the data subjects**
- (where applicable) **processors** and **external IT service providers**

When integrating the data protection officer into the DPIA team, it is important that they can only be involved in an advisory capacity, and in monitoring the implementation of the DPIA.

It makes sense to integrate the specialist departments that conduct the envisaged processing or are meant to use its results, including their staff members, because these often have the deepest insights into the processing, its context, involved data subjects, other stakeholders, and the risks.

It is advisable to integrate the works council (if one exists), because employees – of the organization itself as well as its subcontractors, suppliers, service providers, etc. – regularly feature among the data subjects. The same is true for representatives of other groups of data subjects (e. g. patient council or family council in a care home). In specific cases, it is also conceivable to invite individual data subjects (e. g. in the

form of focus groups) to a DPIA, although the degree of representativeness of the invited persons should be considered. On the one hand, statistical representativeness in the sense of a cross-section of the affected groups is likely difficult to achieve in most cases, and would only have limited value in any case: it would not be permissible to ignore high risks just because the invited data subjects have not spotted them. Even without a representative cross-section, it is possible to obtain good ideas for risk mitigation, a deeper understanding of possible acceptance problems and of major challenges and risks to the data subjects. However, if only distinctly unrepresentative individuals are invited, the question may arise as to whether these can adequately reflect the perspectives of different data subject groups, or whether the intention is to generate a specific outcome.

If important processing operations are performed externally, or important parts of the IT infrastructure are provided by external parties, it may be advisable – as far as possible – to include representatives of these service providers in the DPIA. As described in Chapter 1.3.3, processors are obliged to assist the controller in any case with the DPIA.

### 6.1 Method

The execution phase has three objectives:

- Assess the risks of the envisaged processing to the rights and freedoms of natural persons (Article 35(7)(c) GDPR)
- Select mitigation measures (safeguards, security measures) to address these risks and to ensure the protection of personal data (Article 35(7)(d) GDPR)
- Assess the necessity and proportionality of the envisaged processing operations in relation to the purposes, thus completing the process of assessing necessity and proportionality according to Article 35(7)(b) GDPR (see Chapter 2.4)

It is usually expedient to conduct the risk assessment within the framework of one or more participatory workshops, which bring together the entire DPIA team including possible data subject representatives.

The materials compiled in the preceding Phases I and II serve as the informational basis for the risk assessment. The workshop participants should be provided with the materials beforehand. It is useful to validate the information at the beginning of the workshop and to supplement this where necessary, so that it can be assumed that all the participants share a common understanding. In particular, it should be checked at the outset whether all the categories of data subjects and stakeholders have been identified.

### 6.2 What are risks as defined in the GDPR?

The GDPR does not define the term risk. The short paper No. 18 of the Data Protection Conference derives the following definition from Recitals 75 and 94 of the GDPR:

*A risk in the sense of the GDPR is the existence of the possibility that an event occurs which in itself constitutes a damage (including unjustified interference with the rights and freedoms of natural persons) or that may result in further damage to one or more natural persons.*

*It has two dimensions: first, the severity of the damage, and second, the likelihood that the event and the resulting damages occur.<sup>14</sup>*

This definition raises three questions: What are “damages” (including “unjustified interference with the rights and freedoms”), what are “events”, and how are the severity and likelihood of damages to be assessed? The first two questions are addressed

in the next two sections 6.2.1 and 6.2.2; section 6.4 deals with the assessment of the damage severity and likelihood.

### Damages and interference with rights and freedoms

In European law, the term “rights and freedoms of natural persons” encompasses all the fundamental rights and freedoms found in the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.<sup>15</sup> Article 35 GDPR requires an assessment of the risks where processing is likely to result in an infringement of fundamental rights or could itself violate them.

This abstract formulation makes it difficult to grasp the task of Article 35 GDPR. Fortunately, Recital 75 GDPR operationalizes the concept of risks to rights and freedoms using the more concrete term of damage: Accordingly, a risk to rights and freedoms can be presumed if the processing is likely to result in damages to natural persons. In accordance with the Data Protection Conference’s definition of risk cited above, one must primarily look for damages in order to identify and mitigate the abstract risks to rights and freedoms.

Recital 75 distinguishes between physical, material, and non-material damages. All three categories must be considered in the DPIA.

Examples of how a lack of data protection can result in **physical damages** include incorrect data or processing that leads to the wrong medical treatment. This applies equally if breaches of confidentiality (e.g. address data or data about religion, health, political opinions, sexual orientation, or criminal offenses) abet violent crimes including stalking. Psychological damages can also fall under physical damages, e.g. anxiety, depression, and other psychological damages due to loss of confidentiality or unjustified surveillance.

**Material damages** are primarily economic. There are many conceivable economic damages that can be triggered by data protection violations (including incorrect data/processing). Examples include career disadvantages (illegitimate performance and behavioral control, missed recruitment or promotion opportunities, warning letters, job losses, etc.), curtailed state benefits (e.g. unemployment benefits, housing benefits, welfare benefits), discrimination (e.g. when taking out insurance policies or looking for accommodation), identity theft and fraud, extortion based on confidential data, other financial losses, loss or falsification of evidence (e.g. in a court case or in the context of having to prove that services were provided in a work context), loss of acquired advantages and benefits (e.g. bonus programs, purchased goods or services), unjustified fees or fines, as well as additional expenses in terms of time and money caused by data protection violations (e.g. to unfreeze a bank account or clarify processing errors, including the costs for possible legal advice) and many others.



**Non-material damages** may be of a social, personal, and legal nature. This category is very diverse. It is therefore helpful to create four subcategories:

- **Social disadvantages.** These include damages to reputation, loss of reputation and varying degrees of humiliation (from embarrassment through loss of face up to serious public humiliation or defamation), mobbing, social discrimination, curtailment of social inclusion for instance through (unjustified) blocking of accounts or incorrect data (e. g. age, being included on exclusion orders).
- **Damage to privacy** primarily describes when a person experiences a “creepy” lack of control over their own data and the feeling of being “spied on”, for instance due to video surveillance, biometric recognition, profiling, tracking via websites, end devices and applications or the publication, mention of or reference (e. g. in advertising) to private, intimate details such as address, pregnancy, state of health, sexual or political orientation, religion, etc.
- **Chilling effects** describe a state in which persons refrain from exercising their rights (e. g. to express political opinions) or expressing their (legitimate) personal development (e. g. by visiting certain places) because they fear negative consequences. Chilling effects are a threat above all in the case of data processing operations that constitute unjustified surveillance.
- **(Unjustified) interference with rights.** Any processing of personal data is per se an interference with the fundamental right to personal data protection. It therefore requires a legal basis. Processing operations that take place without sufficient legal basis constitute direct damage, even if they do not result in any other, more “concrete” damages. The same applies to processing operations that go against the principles of data protection (Article 5 GDPR), that do not implement the rights of data subjects or do so insufficiently (Articles 12–22 GDPR), or that do not comply with the GDPR in some other way: They all constitute a violation of the right to informational self-determination and therefore a damage. Data processing operations may also violate other fundamental rights or result in their violations, e. g. the fundamental right to non-discrimination or freedom of expression.

As these remarks show, there are a multitude of potential damages that can result from today’s data processing operations. This is hardly surprising given the ongoing digitization of every area of life. This explains the length and diversity of the list on the one hand, but also makes it clear, on the other hand, why a DPIA is often useful.

#### **Practical tip** Comprehensive analysis

It is important to think through your own data processing operations carefully to identify the possible occurrence of relevant damages and scenarios. A comprehensive view should be taken without being too intimidated by, or shying away from the workload involved – which may seem very large at first sight.

## Events

“Events” are the causes triggering the occurrence of a damage (i.e. that lead to the “realization of the risk”). Commonly, these are likely to be due to non-compliance with the data protection principles (Article 5(1) GDPR), failure to grant the rights of data subjects (Articles 12–22 GDPR) or other infringements of the GDPR (e.g. unjustified data transfers abroad). Typical events are:<sup>16</sup>

- unauthorized or unlawful processing
- processing contrary to the principles of fairness and transparency
- processing that is non-transparent for the data subjects
- unauthorized disclosure of, and access to, data
- accidental loss, destruction, or damage of data
- denial of the rights of data subjects
- utilization of the data by the controller for incompatible purposes
- processing of data that was not foreseen
- processing of incorrect data
- incorrect processing (technical faults, human error)
- processing after the designated storage period
- the processing itself, if the damage is due to the execution of the processing (e.g. because this is illegitimate/lacks a legal basis)

## 6.3 Risk assessment using the protection goals and damage scenarios

The The Standard Data Protection Model (SDM) recommended by the Conference of the Independent German Federal and State Data Protection Supervisory Authorities condenses and systematizes all the requirements of the GDPR in the form of seven protection goals. These are described in detail in the Annex and are only listed here:

- Data minimization
- Availability
- Integrity
- Confidentiality
- Unlinkability
- Transparency
- Intervenability

The SDM’s catalogue of reference measures assigns specific technical and organizational measures to each data protection goal, which are intended to ensure compli-

ance with the goal and the underlying requirements of the GDPR, and prevent the occurrence of damages.

A two-step method is helpful to identify how, by whom or what, and under what conditions damages could be caused to the data subjects and compliance with the data protection goals could be jeopardized. In the first step, concrete damage scenarios are developed and analyzed based on the identified data subjects, the description of the processing operations and other information on the nature, scope, context, and purposes of the processing. To take a systematic approach, for each identified group of data subjects, it should be asked to what extent the actions of the stakeholders or other events (e. g. technical malfunctions, force majeure) could result in physical, material, or non-material damage. It should also be identified, for each scenario, which data protection goals are affected. Chapter 6.3.1 describes a method for developing and analyzing damage scenarios.

The second step starts from the data protection goals. For each goal, the question is asked to what extent the actions of the stakeholders or other events could result in a breach of the protection goal, and what damages could occur for data subjects (besides the data protection violation, which constitutes a damage in itself).

#### **Practical tip** Risk analysis

At first sight, it might seem redundant to conduct the risk analysis in this “two-step” fashion. In fact however it offers three advantages: first, it makes it easier to involve persons without in-depth knowledge of data protection (e. g. employees of specialist departments, data subjects and their representatives). Where exactly in a processing operation the risk of damage-triggering events lies depends on the details of the respective nature and context of the processing. It is often the employees of specialist departments entrusted with planning or performing the processing on a daily basis who have the best insight here: for persons without training in data protection law, however, it is often more intuitive to determine risks using concrete damage scenarios than to approach this using the data protection goals.

Second, compliance with the GDPR can be more reliably ensured by an analysis from the perspective of the data protection goals, because these systematically operationalize the requirements of the GDPR. At the same time, the analysis of compliance with the data protection goals benefits from detailed knowledge of the processing and its exact context, which is uncovered and summarized when developing concrete scenarios.

Third, risk identification and analysis always contain a certain creative element. This is why it is useful to approach it from different viewpoints.

## Creating damage scenarios

In order to create damage scenarios, it is helpful to answer three overarching questions:<sup>17</sup>

1. What damages could occur for the identified data subjects based on the envisaged processing or the data to be processed?
2. What actions and circumstances can result in the respective damage? Which stakeholders are involved and how? Are non-human risk sources relevant, e. g. technical malfunctions?
3. What safeguards are already in place or are planned?

To ensure a systematic approach, the different categories and subcategories of damage (physical, material, non-material etc.) should be worked through for each identified group of data subjects and stakeholders. One should ask whether and how the data processing could lead to damages for the data subjects, and which stakeholders would be involved in this and how.


In this context, it is helpful to ask what information about the data subjects can be deduced from the collected data, and what stakeholders could be interested in this information. It should also be asked whether processing errors (incorrect data or processing), technical malfunctions or force majeure could trigger damages. In any case, the specific trigger (the factor that causes the event) should be identified so that measures can subsequently be implemented to deal with it. It should also be documented which data protection goal(s) is/are affected in the respective scenario.

Some mitigation measures have almost always been already implemented or planned for both envisaged and ongoing processing operations. These measures should be incorporated into the damage scenarios. It is important to differentiate clearly between already implemented and merely planned measures.

The following information should be determined for each damage scenario:

- Description of the scenario
- Data subjects
- Personal data
- Involved actors/stakeholders
- Possible damage for the data subjects
- Elements triggering the damage
- Data protection goals affected
- Any already existing technical and organizational measures

The scenarios formed should be recorded in written form, e. g. in a scenario table as



Scenario No.	Description of the scenario	Data subjects	Personal data	Involved actors (stakeholders)	Possible damage for the data subjects	Elements triggering the damage	Already existing technical & organizational mitigation measures	Data protection goals affected	Severity of the damage	Likelihood	Risk assessment	Additional mitigation measures or enhancement of existing measures
1												
2												

Figure 2: Scenario table

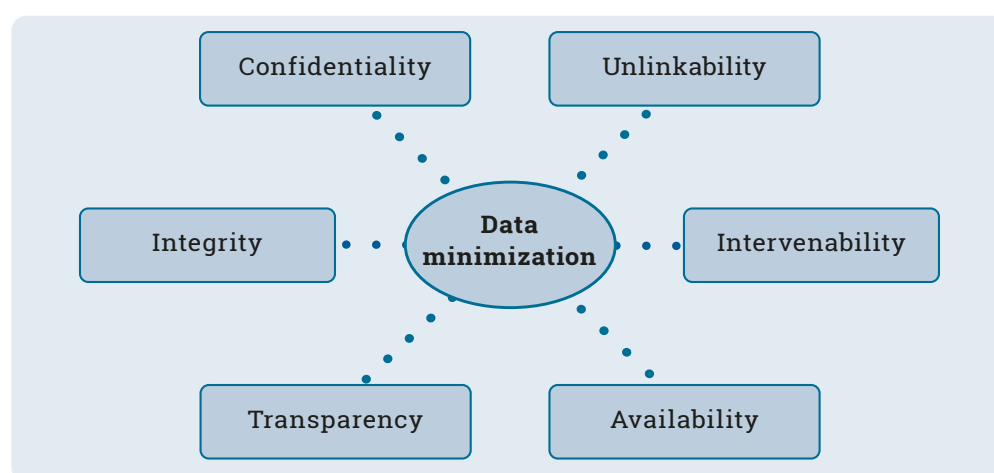
shown in Figure 2. The risk assessment conducted in the next steps and the selected mitigation measures can also be recorded in the table. The value of the table is that it breaks down the scenarios into their key components and provides a clear overview.

### Analysis based on the data protection goals

The next step is to complete the identification and analysis of the risks using the data protection goals. For each data protection goal, the following questions should be answered in relation to each category of data subject:

1. Does the currently envisaged design of the processing ensure compliance with the respective data protection goal?
2. Under what circumstances is a breach of the data protection goal realistically possible? To which stakeholders or non-human risk sources would the breach be attributable – what would be the triggers?
3. What additional damages – beyond the violation of the data protection requirement represented in the data protection goal – are which data subjects likely to suffer as a result of violating the protection goal?

When analyzing the data protection goals – and when selecting measures later – it is important to note that some of the protection goals stand in structurally inherent tension to one another. Depending on the system design and context, for example, “more” intervenability might mean “less” integrity, better availability might mean weaker confidentiality, or higher transparency lower unlinkability and vice versa. This tension is indicated in the star-shaped diagram of the data protection goals (Figure 3). If several data protection goals are affected in one damage scenario and there are tensions between them, it is important to analyze which of the goals should be given priority from the viewpoint of the data subjects. This is important to be able to select the most appropriate mitigation measures to protect the rights and freedoms of data subjects at a later stage.



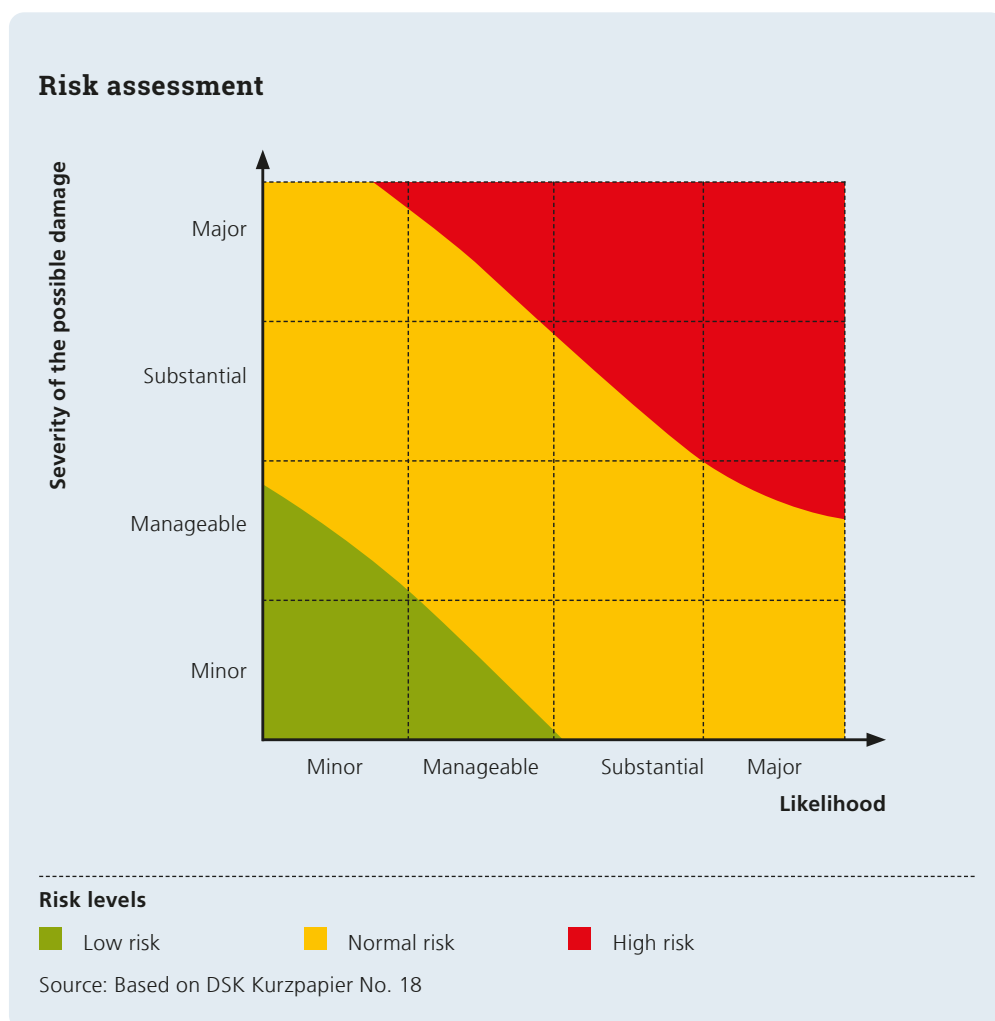
**Figure 3:**  
Data protection goals

## 6.4 Risk assessment

Once the risks have been documented and analyzed by examining the damage scenarios and the data protection goals, they must be assessed. Risks are typically classified into three levels: **low**, **normal**, and **high**.

The level of risk results from the **severity of damage** and the **likelihood** of events occurring that trigger the damage or constitute the damage in themselves. To classify the severity and likelihood of damage, the Data Protection Conference suggests using a four-tier scale: **minor**, **manageable**, **substantial**, and **major**. The risk matrix shown in Figure 4 illustrates these relationships.

As a rule, in data protection neither the severity of damage nor the likelihood of its occurrence can be meaningfully quantified. Instead, one should offer and document a valid and reasonable argumentation for how one decides to scale the different risks in terms of their likelihood and severity, based on the most objective criteria possible.



**Figure 4:**  
Risk matrix

The severity of the damage results from the physical, material, or non-material effects on data subjects. The reversibility of the damage should also be considered here (the more difficult, or costly in terms of time, money or effort, that reversibility is, the more severe the damage). Relevant too is the difficulty data subjects would face if they wanted to withdraw from the processing (including if they do not know about the processing in the first place), and how easy or difficult it would be for them to examine the processing themselves or have it examined in court. The more persons are “at the mercy” of processing, the greater the severity of possible damages connected to the processing.

To assess the likelihood, it is useful to consider the motives and capabilities of the stakeholders as well as the effort needed to trigger the risk event and the robustness of existing mitigation measures.

## 6.5 Selection of mitigation measures

Once the risks have been analyzed and assessed, they must be appropriately addressed, i.e. mitigated or eliminated completely if possible. In most cases, this is done by selecting and implementing technical and organizational measures. Alternatively, the processing can be modified or even discontinued.

Article 35(7)(d) GDPR requires the controller to “address” the risks and demonstrate that the processing complies with the GDPR. “Address” is generally understood to mean “reduction” or “mitigation”. At the very least, all the risks assessed as “high” must be reduced to the extent that they only still qualify as “normal”, although this always raises the question why “normal” risks are not reduced to “low”, if suitable measures are available. This should be justified on a case by case basis.

During the risk assessment, for each identified risk, it must be documented what factors exactly could lead to the risk materializing (or what the triggering elements are), and which protection goals are affected by it. This can then be used as a basis for selecting suitable measures. These can be both technical and organization in kind. It may not always be necessary to implement additional measures – sometimes it can make more sense to enhance existing measures.

Measures can be prioritized according to the severity of the risks. It is not permissible to assess measures only from the viewpoint of their costs and simply accept high risks, because the required mitigation measures are deemed too expensive. Neither is it permissible to accept high risks because the number of data subjects affected is considered to be small.

The lists of typical mitigation measures featured in the Standard Data Protection Model (SDM) can help in selecting appropriate measures, as can the Catalogue



of Reference Protection Measures in the SDM – currently a work in progress. The Catalogue of Reference Measures is divided into modules that each describe generic measures for different data protection requirements (e. g. logging, separation, erasure, and destruction etc.). For each module, it is specified which data protection goals can be addressed using the measures described in the module. The SDM itself contains a list of generic measures structured according to the protection goals. Additional guidance is provided by the “Knowledge Bases” document of the French Data Protection Authority CNIL, and the Guide to Basic Protection based on the “IT-Grundschrift” (“IT baseline protection”) developed by the German Federal Office for Information Security (BSI).

#### **Practical tip** Lists of typical mitigation measures

Standard Data Protection Model V.2, Section D

[https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode\\_V2.0.pdf](https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V2.0.pdf)

Catalogue of Reference Measures of the Standard Data Protection Model with modules

<https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>

IT Security Compendium of the German Federal Office for Information Security (BSI)

[https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium\\_node.html](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html)

CNIL Privacy Impact Assessment: Knowledge Bases:

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>

## 6.6 Assessment of the remaining risks and decision about further steps

In this step, it must be assessed whether the selected measures reduce the identified risks to an acceptable level. If high risks remain despite the selected measures, other additional protective measures must be selected until the risks in question are sufficiently mitigated, or the data protection supervisory authority must be consulted in line with Article 36 GDPR (cf. Chapter 6.10), or the processing must be abandoned. This fundamental decision must be made by the controller.

In any case, the processing may not be approved and may not go ahead as long as high risks remain.

## 6.7 Assessment of necessity and proportionality

Based on the assessment of (remaining) risks and the materials compiled in the preceding phases, the necessity and proportionality of the processing operations in relation to the purposes can then be assessed as required under Article 35(7)(b) GDPR. It is important that sufficient reasons for why precisely this kind of data processing is required have been documented. The following criteria must be fulfilled:

1. Lawfulness of processing as set out in Article 6(1) GDPR is ensured
2. The principles of data protection as described in Article 5(1) GDPR are effectively discharged
3. All the other requirements of the GDPR (e. g. complying with the rights of data subjects) are fulfilled and the protection of personal data is ensured
4. All the risks are sufficiently mitigated and there is no longer any high risk to the data subjects

## 6.8 Recommended method: Participatory workshop-based method

Provided the requirements described in Chapter 1.2 are satisfied, the controller may freely decide how to carry out the DPIA. In particular for Phase III (execution phase), which forms the core of the DPIA, the DPIA method described in this handbook recommends a participatory workshop-based approach. The reason for this is that much of the information required for the DPIA about the envisaged processing, the IT systems and business processes as well as the data subjects and other stakeholders is already present in the organization, but often not in documented form – rather as an intuitive understanding of the processing context in the heads of employees.

This information, which is often dispersed throughout the organization, must be systematically collected, and prepared for the DPIA. This is often best-done using interviews and one or more participatory workshops, in which the DPIA team gather the information together with representatives of the relevant organizational units and – if possible – the data subjects or their representatives, and identify, analyze, and assess risks and discuss adequate mitigation measures.

As an example, a specific PIA could proceed as follows: Individual experts or a small core team conduct the threshold assessment in Phase I and compile the documentation and information in Phase II, possibly based on interviews with employees of the respective specialist departments. The entire DPIA team – including possible data subject representatives – then come together in Phase III in one or more workshops, to validate the information compiled in Phase II and to perform the risk identification, analysis, and assessment in a participatory, dialogue-based process. This workshop should integrate consultation with data subjects if possible.

Concrete suggestions for mitigation measures and, in particular, adjustments to the envisaged processing (e. g. using cryptographic methods, roles and rights models, reducing the processing of personal data in the sense of data minimization) will usually have to be made by experts. However, it is sensible to discuss the possible measures in the workshop as well, since their practical applicability and effectiveness are influenced by the context of the respective business processes and workflows in which they should take effect. The employees of the affected specialist departments (e. g. the carers in a healthcare context) can provide important input here.

## 6.9 DPIA report

The preparation of the DPIA report completes the execution phase of the DPIA. Producing such a report is part of the general accountability obligations of the controller in accordance with Article 5(2) GDPR. In line with Article 58(1)(a) GDPR, the report must be presented upon request to the data protection supervisory authority. It is up to the controller to decide about further disclosure (e. g. on a company website). However, since disclosure can enhance transparency and thus confidence in processing operations (and ultimately in the organization as a whole), it should be considered, and is even recommended by the Article 29 Data Protection Working Party.<sup>18</sup> Obviously, any trade secrets or information that could be misused as the basis for an attack on the controller can be removed from the published version of the report. However, what should not happen is that the published report conceals problematic facts, so that a distorted or false impression of the processing operation and its risks is created.

The report is also needed to conduct Phases IV and V of the DPIA (Implementation and Sustainability).

The report should follow a clear structure and contain the following information:

1. Description of the processing operations in line with Article 30 GDPR
2. Further information and documentation of the processing operations and their contexts
3. Documentation of the legal basis according to Article 6(1) GDPR
4. Results of the risk evaluation (identification, analysis, assessment of risks)
5. Measures selected to mitigate the risk
6. Information about any remaining risks, including their justification

## 6.10 Prior consultation of the supervisory authorities

If the evaluation of the residual risks reveals that high risks remain that the controller cannot mitigate using further measures, the processing must either be abandoned or the responsible supervisory authority consulted. This obligation is regulated in Article 36 GDPR. According to Article 36(3) GDPR, the controller must provide the supervisory authority with the following information:

- (where applicable) information about the responsibilities of the controller and any joint controllers or processors (Article 36(3)(a) GDPR)
- purposes and means of the intended processing (Article 36(3)(b) GDPR)
- (information about) the planned measures and safeguards (Article 36(3)(c) GDPR)
- (where applicable) contact details of the data protection officer (Article 36(3)(d) GDPR)
- the report and any other documentation concerning the DPIA (Article 36(3)(e) GDPR)
- any other information requested by the supervisory authority (Article 36(3)(f) GDPR)

The supervisory authority must provide the controller with the relevant written advice (e. g. concerning possible additional measures) within 8 weeks after receipt of the request for consultation. For complex processing operations, the supervisory authority may extend this period by a further six weeks.

### 7.1 Implementing and testing the mitigation measures

If the selected measures and safeguards can mitigate the risks sufficiently and the processing is to be pursued, these measures must now be implemented.

The effectiveness of the measures should be tested and the test results documented. The tests should be conducted regularly based on a test methodology that should be developed after the processing has been approved, and the test results should be recorded. If new risks are identified in this process, these must be dealt with according to the method described in Chapter 6.

### 7.2 Demonstrating compliance with the GDPR and approval of the processing

Once the mitigation measures have been implemented successfully, it becomes possible to demonstrate, in accordance with Article 35(7)(d) GDPR, that the processing meets the requirements of the GDPR as a whole.

With proof of compliance with the GDPR as a whole, the processing can finally be approved by the controller and go ahead.

## 8 Phase V: Periodic review of the DPIA

After completing a DPIA cycle, suitable measures must be taken to ensure its sustainability. These include monitoring the risks, regular checks and adjustments of the DPIA in the context of changes, if these changes are relevant to the risks associated with the processing operations (Article 5(2), Article 35(11), Article 39(1)(b) GDPR).

The DPIA report serves as the basis for such monitoring, especially the documentation it contains on the risks, mitigation measures and associated test methodologies and test records. Any detected risks and, where applicable, any changes that have occurred should be reliably identified and the effectiveness of mitigation measures regularly reviewed. If there are larger deviations with regard to the effectiveness of mitigation measures or major changes to the processing, Phases II to IV of the DPIA should be repeated.

Any adjustments made in the context of risk assessment, mitigation measures and the test methodology as well as the processing itself are to be documented in the DPIA report.

To ensure reliable monitoring of the DPIA, it makes sense to integrate this into a general data protection management system, as described in the Standard Data Protection Model Part D, or to set up such a system. Ensuring sustainability and conducting continuous assessments is the responsibility of the controllers, or a third party commissioned by them, assisted where necessary by members of the DPIA team and (in an advisory capacity) the data protection officer.

### A Description of the protection goals

In the field of IT-security, protection goals (German: Schutzziele or Gewährleistungsziele) have, for many years, been used to operationalize security requirements. Therefore, it is also helpful to use them for DPIAs. In recent years, in addition to the three established IT-security protection goals (confidentiality, integrity and availability), three further protection goals have been formulated that are more closely related to data protection, to operationalize the related data protection principles: Transparency, as a precondition for the data subject and other stakeholders to be able to understand and control processing operations; unlinkability, as a precondition for purpose limitation and necessity; and intervenability, as a precondition for the exercise of data subject rights. Together, these six protection goals fully cover the data protection principles outlined in Art. 5 GDPR (cf. Table 1). They form part of the Standard Data Protection Model recommended by the Conference of the Independent German Federal and State Data Protection Supervisory Authorities. To help further concretize the protection goals, measures by which they might be realized have been defined, for different levels (data, systems, processes). The protection goals thus translate the abstract normative requirements of Art. 5 GDPR into concrete functional requirements. This supports the practical conduct of a DPIA, as they directly relate to the functionality and implementation of the processing operation that is to be assessed in the DPIA. The following explanations are an abridged version of the English-language text of the SDM.

#### A.1 Data minimization

The protection goal Data minimization covers the fundamental requirement under data protection law to limit the processing of personal data to what is appropriate, substantial and necessary for the purpose (Data minimization). The implementation of this minimization requirement has a far-reaching influence on the scope and intensity of the protection concept determined by the other protection goals. Data minimization specifies and operationalizes the principle of necessity in the processing process, which requires from this process as a whole as well as each of its steps not to process more personal data than is needed to achieve the purpose of processing. The minimi-

Protection Goal	Requirements of the GDPR
Data minimization	Data minimization (Art. 5(1) (c) GDPR)
	Storage limitation (Art. 5(1) (e) GDPR)
	Data protection by design and by default (Art. 25(2) GDPR)
Availability	Availability (Art. 32(1) (b) GDPR)
	Resilience (Art. 32(1) (b) GDPR)
	Ability to restore availability (Art. 32(1) (b) (c) GDPR)
	Measures to rectify personal data breaches and mitigate their effects (Art. 33 (3) (d), Art. 34(2) GDPR)
Integrity	Accuracy (Art. 5(1) (d) GDPR)
	Integrity (Art. 5(1) (f), Art. 32(1) (b) GDPR)
	Prevention of errors and discrimination in profiling (Art. 22(3) (4) in connection with Recital 71 GDPR)
	Resilience (Art. 32(1) (b) GDPR)
	Measures to rectify personal data breaches and mitigate their effects (Art. 33 (3) (d), Art. 34(2) GDPR)
	Suitable monitoring of the processing (Art. 32, 33, 34 GDPR)
Confidentiality	Confidentiality (Art. 5(1) (f), Art. 28(3) (b), Art. 29, Art. 32(1) (b), Art. 32(4), Art. 38(5) GDPR)
	Resilience (Art. 32(1) (b) GDPR)
	Measures to rectify personal data breaches and mitigate their effects (Art. 33 (3) (d), Art. 34(2) GDPR)
Intervenability	Facilitating the exercise of data subject rights (Art. 12(2) GDPR)
	Identification and authentication (Art. 12(6) GDPR)
	Means to rectify inaccurate data (Art. 5(1) (d), Art. 16 GDPR)
	Erasure of data (Art. 17(1) GDPR)
	Scope to restrict processing of data (Art. 18 GDPR)
	Data portability (Art. 20(1) GDPR)
	Scope to intervene in processes of automated decision making (Art. 22(3) GDPR)
	Data protection by design and by default (Art. 25(2) GDPR)
	Measures to rectify personal data breaches and mitigate their effects (Art. 33 (3) (d), Art. 34(2) GDPR)
	Consent management (Art. 4 No. 11, Art. 7(4) GDPR)
	Implementation of orders of the supervisory authorities (Art. 58(2) (f) and (j) GDPR)

**Table 1:**

Systematization of the legal requirements by means of the protection goals (Quelle: SDM 2.0a (2019), p. 28–29)



Unlinkability	Purpose limitation (Art. 5(1) (b) GDPR)
Transparency	Transparency for the data subjects (Art. 5(1) (a), Art. 12(1) and (3), Art 15, Art. 34 GDPR)
	Accountability and capacity to demonstrate compliance (Art. 5(2), Art. 7(1), Art. 24(1), Art 28(3) (a), Art. 30, Art. 33(5), Art. 35, Art. 58 (1) (a) and (e) GDPR)
Testing, assessment and evaluation (Art. 32(1) (d) GDPR) is to be implemented as a process that includes all requirements.	

zation requirement applies not only to the quantity of data processed, but also to the scope of its processing, its storage period and its accessibility. In particular, it is necessary to ensure that personal data are kept only in a form which permits identification of data subjects for as long as is necessary for the purposes of the processing (Storage limitation). Data minimization starts with the design of the information technology by the manufacturer through its configuration and adaptation to the operating conditions (Data protection-friendly default settings) to its use in the core processes of processing as well as in the supporting processes, for example in the maintenance of the systems used.

The protection goal Data minimization can be achieved by:

- Reduction of recorded attributes of data subjects
- Reduction of processing options in each processing step
- Reduction of the possibility of gaining knowledge of existing data
- Establishing default settings for data subjects which limit the processing of their data to what is necessary for the purpose of the processing
- Preference for automated processes (not decision processes), which make it unnecessary to gain knowledge of processed data and limit influence in comparison to dialogue controlled processes
- Implementation of data masks that suppress data fields, and automatic blocking and erasure routines, pseudonymisation and anonymisation processes
- Definition and implementation of an erasure concept
- Rules for the monitoring of processes to change processing activities

## A.2 Availability

The protection goal Availability refers to the requirement that access to personal data and their processing is possible without delay and that they can be used properly in the intended process. For this purpose, the data must be accessible by authorized parties and the intended methods for processing must be applied to them. Availability includes the concrete retrievability of data, e.g. through data management systems, structured databases and search functions, and the ability of the technical

systems used to present data appropriately for humans (Availability). Furthermore, measures must be taken to implement availability to ensure that personal data and access to them can be rapidly restored in the event of a physical or technical incident (Recoverability). Measures must also be implemented to guarantee the availability of personal data and the systems and services that process them when they are under a reasonable expected load and to ensure that the protection of personal data is not compromised in the event of an unexpectedly high load (Resilience). If, in exceptional cases, the protection of personal data with regard to availability is nevertheless violated, it must be ensured that measures are taken to rectify and mitigate the violation (Rectification and mitigation of data protection breaches).

Typical measures to guarantee Availability are:

- Creation of backup copies of data, process states, configurations, data structures, transaction histories, etc. according to a tested concept
- Protection against external influences (malware, sabotage, force majeure)
- Documentation of data syntax
- Redundancy of hardware, software and infrastructure
- Implementation of repair strategies and avoidance processes
- Preparation of an emergency concept for restoring processing activity
- Representation arrangements for absent employees

## A.3 Integrity

The protection goal Integrity refers, on the one hand, to the requirement that information technology processes and systems continuously comply with the specifications that were defined for them to perform their intended functions (Integrity). On the other hand, integrity refers to the property that the data to be processed remain intact (Integrity), complete, correct and up-to-date (Correctness). Deviations from these characteristics must be excluded or at least detectable (Adequate monitoring of processing) so that they can be taken into account and corrected (Rectification and mitigation of data protection breaches).

This also applies if the underlying systems and services are subject to unexpectedly high loads (Resilience). In addition to the aspect of freedom from errors, the aspect of freedom from discrimination must be maintained, especially in automated evaluation and decision-making processes (Freedom from errors and discrimination). The factors and characteristics of an assessment or decision-making process that may have potentially discriminatory effects shall be identified a priori in the legal review, taken into account in implementation and monitored in operation. This aspect is reflected, for example, by measures to clean up training data and validate results when applying AI procedures.

Typical measures to safeguard integrity or to assess a breach of integrity are:

- Restriction of writing and modification rights
- Use of checksums, electronic seals and signatures in data processing processes in accordance with a cryptographic concept
- Documented assignment of authorizations and roles
- Erasure or rectifying of incorrect data
- Hardening of IT systems so that they have no or as few secondary functionalities as possible
- Processes for maintaining the timeliness of data
- Processes for identification and authentication of persons and equipment
- Definition of the target behavior of processes and regular performance of tests to determine and document functionality, risks, security gaps and side effects of processes
- Determination of the target behavior of processes and procedures and regular performance of tests to ascertain or determine the actual states of processes
- Protection against external influences (espionage, hacking)

## A.4 Confidentiality

The protection goal Confidentiality refers to the requirement that no unauthorized person can access or use personal data (Confidentiality). Unauthorized persons are not only third parties outside the responsible body, but also employees of technical service providers who do not require access to personal data in order to provide the service, or persons in organizational units who have no connection whatsoever with the content of a processing activity or with the data subject. The confidentiality of personal data must also be ensured when the underlying systems and services are subject to unexpectedly high loads (Resilience). Should confidentiality nevertheless be violated in exceptional cases, it must be ensured that measures are taken to remedy and mitigate the accompanying violation of the protection of personal data (Remedy and mitigation of data protection violations).

Typical measures to guarantee confidentiality are:

- Definition of an authorization and role concept according to the necessity principle on the basis of identity management by the responsible body
- Implementation of a secure authentication procedure
- Limitation of authorized personnel to those who are verifiably responsible (locally, professionally), qualified, reliable (if necessary with security clearance) and formally approved, and with whom no conflict of interests may arise in the exercise of their duties
- Specification and monitoring of the use of authorized resources, in particular communication channels, specified environments (buildings, rooms) equipped for processing activities

- Definition and monitoring of organizational processes, internal regulations and contractual obligations (obligation to maintain data secrecy, confidentiality agreements, etc.)
  - Encryption of stored or transferred data and processes for managing and protecting cryptographic information (cryptographic concept)
- Protection against external influences (espionage, hacking)

## A.5 Unlinkability

The protection goal Unlinkability refers to the requirement that personal data shall not be merged, i.e. linked. It must be implemented in practice especially if the data to be merged were collected for different purposes (Purpose limitation). The larger and more meaningful the data base, the greater the potential greed may be to use the data beyond the original legal basis. Such further processing is only legally permissible under strictly defined circumstances. The unlinkability is to be ensured by means of technical and organizational measures. In addition to measures for pseudonymization, other measures that allow further processing separately from the original processing are also suitable, both on the organization side and on the system side. The data base can be adapted, for example, by authorization systems and reduction to the extent necessary for the new purpose.

Typical measures to guarantee unlinkability are:

- Restriction of processing, use and transfer rights
- Program-wise omission or closure of interfaces in processing methods and components
- Regulatory measures to prohibit backdoors and quality assurance audits for compliance in software development
- Separation according to organizational/departmental boundaries
- Separation by means of role concepts with graduated access rights on the basis of identity management by the responsible body and a secure authentication process
- Approval of user-controlled identity management by the controller
- Use of purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymized data
- Regulated processes for purpose amendments

## A.6 Transparency

The protection goal Transparency refers to the requirement that both data subjects (Transparency for data subjects) and system operators (Adequate monitoring of processing) and competent supervisory bodies (Accountability and verifiability) shall be able to identify to varying degrees which data are collected and processed when and

for what purpose in a processing activity, which systems and processes are used to determine where the data are used and for what purpose, and who has legal responsibility for the data and systems in the various phases of data processing. Transparency is necessary for the monitoring and control of data, processes and systems from their creation to their erasure and a prerequisite for legally compliant data processing and to which, where necessary, data subjects can give an informed consent (Consent management). Transparency of the whole data processing and of the instances involved can help to ensure that, in particular, data subjects and supervisory bodies can identify deficiencies and, if necessary, demand appropriate changes to the processing.

Typical measures to guarantee transparency are:

- Documentation in the sense of an inventory of all processing activities in accordance with Art. 30 GDPR
- Documentation of the components of processing activities, in particular business processes, databases, data flows and network plans, IT systems used for this purpose, operating procedures, descriptions of processing activities, interaction with other processing activities
- Documentation of tests, of the release and, where appropriate, the data protection impact assessment of new or modified processing activities
- Documentation of the factors used for profiling, scoring or semi-automated decisions
- Documentation of contracts with internal employees, contracts with external service providers and third parties from whom data is collected or transmitted, business distribution plans, responsibility regulations
- Documentation of consents, their revocation and objections
- Logging of accesses and changes
- Versioning
- Documentation of processing by means of protocols on the basis of a logging and evaluation concept
- Documentation of the data sources, e.g. the implementation of information duties towards data subjects where their data were collected and the handling of data breaches
- Notification of data subjects in the event of data breaches or further processing for another purpose
- Traceability of the activities of the controller for granting data subjects' rights
- Consideration of the information rights of data subjects in the logging and evaluation concept
- Provision of information on the processing of personal data to data subjects

## A.7 Intervenability

The protection goal Intervenability refers to the requirement that the data subjects have the rights to notification, information, rectification (Possibility of rectification of data), erasure (Erasure of data), restriction (Restriction of processing of data), data portability (Data portability), objection and obtaining the intervention in automated individual decisions (Possibility of intervention in processes of automated decisions) are granted immediately and effectively if the legal requirements exist (Support in the exercise of data subjects' rights) and the processing authority is obliged to implement the corresponding measures. Where the data controller has information enabling him to identify the data subjects, he must also take measures to identify and authenticate the data subjects who wish to exercise their rights (Identification and authentication). In order to implement the rights of data subjects and supervisory orders (Implementation of supervisory orders) and to remedy and mitigate data protection breaches (Remedying and mitigating data protection breaches), the controllers must at all times be in a position to intervene in data processing, from collection to erasure of the data. Where the processing of personal data is based on the consent of the data subject, measures must be taken to ensure that the personal data are processed only where the data subject has given his or her consent and where that consent has not been withdrawn (Consent management).

For information technology processing to which the data subjects themselves have access (e.g. applications on the smartphone) and for which different data protection settings are intended, Data Protection by Default must be defined by the controller and further measures must be taken. These further measures must enable data subjects to make their own configurations, differentiated according to the respective processing purposes, and to decide which processing operations they wish to allow that go beyond the minimum required (Data protection-friendly default settings).

Typical measures to guarantee intervenability are:

- Measures for differentiated consent, revocation and objection options
- Creation of necessary data fields, e.g. for blocking indicators, notifications, consents, objections, counterstatements
- Documented processing of faults, problem handling and changes to processing activities as well as to technical and organizational measures
- Possibility of deactivating individual functionalities without affecting the overall system
- Implementation of standardized query and dialogue interfaces for data subjects to assert and/or enforce claims
- Operation of an interface for structured, machine-readable data for the retrieval by data subjects
- Identification and authentication of persons who wish to exercise data subjects' rights

- Establishment of a Single Point of Contact for data subjects
- Operational possibility of compiling, consistently rectifying, blocking and erasure of all data stored on a person
- Provision of options for data subjects in order to be able to set up programs in line with data protection requirements

---

Appendix

---

## B Further literature

Article 29 Data Protection Working Party, "Guidelines with regard to data protection officer", WP 243 rev. 01, Brussels, 5.4.2017.

[https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612048](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048)

—, "Guidelines on data protection impact assessment and answering the question whether a processing in the sense of Regulation 2016/679 "is likely to result in a high risk"", WP 248 rev.01, Brussels, 4.10.2017

[http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

CNIL (Commission Nationale de l'Informatique et des Libertés), „Privacy Risk Assessment: Knowledge Bases“, Paris, 2018.

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>

—, „Privacy Risk Assessment: Templates“, Paris, 2018.

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>

—, „Privacy Risk Assessment: Methodology“, Paris, 2018.

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>

De, Sourya Joyee, and Daniel Le Métayer, Privacy Risks Analysis, Morgan & Claypool, San Rafael, 2016.

ISO/IEC 29134:2017, „Information technology – Security techniques – Guidelines for privacy impact assessment“, Internationale Organisation für Normung (ISO), Genf, 2017.

Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK),

„Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (Version 2.0a)“, 2019.

<https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf>

—, „Datenschutz-Folgenabschätzung nach Article 35 DS-GVO“, Kurzpapier 5, 2017.

<https://www.datenschutzkonferenz-online.de/kurzpapiere.html>

—, „Liste der Verarbeitungstätigkeiten, für die eine DPIA durchzuführen ist“, Version 1.1, 2018.

[https://www.datenschutzkonferenz-online.de/media/ah/20181017\\_ah\\_DSK\\_DPIA\\_Muss-Liste\\_Version\\_1.1\\_Deutsch.pdf](https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DPIA_Muss-Liste_Version_1.1_Deutsch.pdf)

—, „Risiko für die Rechte und Freiheiten natürlicher Personen“, Kurzpapier 18, 2018.

<https://www.datenschutzkonferenz-online.de/kurzpapiere.html>

Mester, Britta, Nicholas Martin, Ina Schiering, Michael Friedewald und Dara Hallinan, Schwerpunktthema „Datenschutz-Folgenabschätzung“, Datenschutz und Datensicherheit (DuD), 3/2020.

Wright, David und Paul De Hert (Hrsg.), Privacy Impact Assessment, Springer, Dordrecht, Heidelberg, London, New York, 2012.



## C Abbreviations

---

Appendix

---

<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>CNIL</b>	Commission Nationale de l'Informatique et des Libertés
<b>DPIA</b>	Data Protection Impact Assessment
<b>GDPR</b>	General Data Protection Regulation
<b>ENISA</b>	European Union Agency for Cybersecurity (formerly: European Network and Information Security Agency)
<b>GPS</b>	Global Positioning System
<b>CFREU</b>	Charter of Fundamental Rights of the European Union
<b>HR</b>	Human Resources
<b>IT</b>	Information Technology
<b>NGO</b>	Non-Governmental Organization
<b>SDM</b>	Standard Data Protection Model

## D Footnotes

1. Friedewald, M.; Bieker, F.; Obersteller, H. et al. (2017): Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz. Dritte, überarbeitete Auflage. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt).
2. The project on which this handbook is based – “Data protection impact assessment for companies and public authorities” (Datenschutz-Folgenabschätzung für die betriebliche und behördliche Praxis) – was supported with funding from the German Federal Ministry of Education and Research under grant nos. 03VP03551, 03VP03552 and 03VP03553. The authors are solely responsible for the contents.
3. Conference of the Independent Data Protection Authorities of the Federal and State Governments of Germany (Datenschutzkonferenz, DSK) (2017): Data protection impact assessment according to Art. 35 GDPR. Short paper 5; DSK (2018): Risks to the rights and freedoms of natural persons, Short paper No. 18.
4. Gonscherowski, S.; Herber, T.; Robrahn, R. et al. (2017). Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO auf der methodischen Grundlage eines standardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines „Pay as you drive“-Verfahrens (V 0.10)
5. DSK (2019). Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele (Version 2.0a).
6. In cases of doubt, other language versions were referred to identify linguistic differences, without making a detailed analysis of those language versions. For readability purposes, the text does not use gender-specific language.
7. For details, see Arning/Rothkegel, in: Taeger/Gabel (Hrsg.), DSGVO/BDSG Kommentar, Art. 4 Rn. 164 ff., although opinions differ and a works council or staff council can also be obliged.
8. E.g. Reibach, in: Taeger/Gabel (Hrsg.), DSGVO/BDSG Kommentar, Art. 35 Rn. 9.
9. Article 29 Data Protection Working Party, Guidelines with regard to data protection officer, WP 243 rev. 01, 5.4.2017, p. 16–17
10. Article 29 Data Protection Working Party, Guidelines on data protection impact assessment and answering the question whether a processing in the sense of Regulation 2016/679 “is likely to result in a high risk”, WP 248 rev.01, 4.10.2017, p. 8

11. DSK (2018): „Liste der Verarbeitungstätigkeiten, für die eine DPIA durchzuführen ist“, [https://www.datenschutzkonferenz-online.de/media/ah/20181017\\_ah\\_DSK\\_DPIA\\_Muss-Liste\\_Version\\_1.1\\_Deutsch.pdf](https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DPIA_Muss-Liste_Version_1.1_Deutsch.pdf).
12. European Data Protection Board (EDPB), Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR), 25.09.2018. Available at: [https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion\\_2018\\_art.\\_64\\_de\\_sas\\_dpia\\_list\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_de_sas_dpia_list_en.pdf) accessed on 16.01.2020.
13. Article 29 Data Protection Working Party, Guidelines on data protection impact assessments, p. 10–13
14. DSK (2018): Risks to the rights and freedoms of natural persons, p. 1.
15. Bieker, F. und Bremert, B. (2020) Identifizierung von Risiken für die Grundrechte von Individuen. Auslegung und Anwendung des Risikobegriffs der DS-GVO, in: Zeitschrift für Datenschutz (ZD) 10(1), p. 7–14.
16. Based on: DSK (2018): Risk to the rights and freedoms of natural persons, p. 3
17. Based on: DSK (2018): Risk to the rights and freedoms of natural persons, p. 2
18. Article 29 Data Protection Working Party, Guidelines on data protection impact assessments, p. 22

## E About the authors

Appendix

### Dr Nicholas Martin

Senior researcher and project manager in the Competence Center for Emerging Technologies at Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe



### Dr. Michael Friedewald

Head of business unit Information and Communication Technologies at Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe; Coordinator of the collaborative research project Forum Privacy and Self-Determination in a Digital World supported by the German Federal Ministry of Education and Research



### Prof. Dr. Ina Schiering

Institute for Information Engineering at Ostfalia University of Applied Sciences; research focus on privacy by design in IoT applications; Coordinator of the research project SecuRIIn supported by the Ministry for Science and Culture of Lower Saxony



### Dr. Britta Alexandra Mester

Lawyer, legal counsel, and head of training programs with datenschutz nord GmbH; lecturer C3L University of Oldenburg; editor, DuD – Datenschutz und Datensicherheit; instructor BBS Wechloy



### Dr. Dara Hallinan

Senior researcher in the research group Intellectual Property Rights in Distributed Information Infrastructures at FIZ Karlsruhe – Leibniz Institute for Information Infrastructure



### Prof. Dr. Meiko Jensen

Professor of IT Security and Privacy at Kiel University of Applied Sciences; Adjunct Associate Professor for Cyber Security at the University of Southern Denmark



According to the EU General Data Protection Regulation (GDPR), a Data Protection Impact Assessment (DPIA) must be performed whenever the processing of personal data is likely to pose a high risk to the rights and freedoms of natural persons. A Data Protection Impact Assessment is a systematic risk analysis that should be conducted before commencing data processing. Its purpose is to help data controllers identify and assess potential dangers, and select and implement suitable mitigation measures.

This manual provides a concise introduction to the requirements of the GDPR relating to the Data Protection Impact Assessment and its objectives. It discusses the necessary preconditions for successfully performing a DPIA and provides a step-by-step guide to the conduct of a DPIA.

#### Contents:

- Data Protection Impact Assessments according to the GDPR
- Phases of a Data Protection Impact Assessment
- Risks as understood by the GDPR
- Identification and assessment of data protection risks

#### Intended Readership:

- Data protection and privacy officers
- Data controllers in private-sector companies and public administration

GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung