



# Data Protection Impact Assessments in Practice

## Experiences from Case Studies

Michael Friedewald<sup>1</sup>(✉) , Ina Schiering<sup>2</sup> , Nicholas Martin<sup>1</sup> ,  
and Dara Hallinan<sup>3</sup> 

<sup>1</sup> Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe, Germany  
{michael.friedewald,nicholas.martin}@isi.fraunhofer.de

<sup>2</sup> Ostfalia University of Applied Sciences, Wolfenbüttel, Germany  
i.schiering@ostfalia.de

<sup>3</sup> FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur,  
Eggenstein-Leopoldshafen, Germany  
dara.hallinan@fiz-karlsruhe.de

**Abstract.** In the context of the project *A Data Protection Impact Assessment (DPIA) Tool for Practical Use in Companies and Public Administration* an operationalization for Data Protection Impact Assessments was developed based on the approach of *Forum Privatheit*. This operationalization was tested and refined during twelve tests with startups, small- and medium sized enterprises, corporations and public bodies. This paper presents the operationalization and summarizes the experience from the tests.

**Keywords:** Data Protection Impact Assessment · Privacy · General Data Protection Regulation · Standard Data Protection Model · Data protection goals · Risk management

## 1 Introduction

A central element of the General Data Protection Regulation (GDPR) is the risk based approach, which is aimed at addressing new technologies and complex services processing personal data. Examples are Internet of Things (IoT), mHealth and mobility applications where various sensors and Artificial Intelligence (AI) approaches are employed. Especially in the area of mHealth applications, special categories of personal data in the sense of Art. 9 GDPR are typically processed. Such services often contain products from several technology providers (hardware and software artifacts) and are composed of cloud services from various providers.

When considering the specific privacy risks in the context of a service, the controller needs to clarify whether the intended processing is likely to result in a high risk to the rights and freedoms of natural persons. In this case a Data Protection Impact Assessment (DPIA) according to Art. 35 (1) GDPR must be conducted. In guidance concerning the severity of privacy risks the Article 29 Data Protection Working Party proposed - in their Guidelines on Data

Protection Impact Assessment - several criteria which serve to define technologies as constituting a high risk: evaluation and scoring, automated-decision making with legal or similar significant effect, systematic monitoring, sensitive data, data processed on a large scale) [2, 14].

The GDPR itself merely provides a minimum standard for carrying out a DPIA, as stipulated by Art. 35(7) GDPR. Accordingly, in recent years, data protection authorities [10, 23], scientific consortia [12, 27], standardisation bodies [25] and trade associations [17] have developed methodological frameworks for carrying out a DPIA. However, these methods differ considerably with regard to the procedure, the process and the interpretation of the abstract requirements of Art. 5 GDPR. As they are very abstract, their concrete implementation in practice is the responsibility of the respective institution.

For a substantial DPIA, the context in particular is very important since it makes a huge difference for the individual whether a service - e.g. a communication or collaboration service - is used in a normal business context or for the processing of health relevant personal data. Finally, the implementation of a DPIA is always a process involving many people - or at least it should be. It is a challenge to introduce people whose background is neither data protection law nor computer science to the questions and evaluation standards that are to be applied for a DPIA. Finally, in addition to the data protection requirements, in many cases there are other important requirements that have to be balanced against each other.

In this regard, we were interested in designing and testing a DPIA process that is generic enough to be used in all possible application areas, but also able to take into account the specifics of each area. The basis for this work was a methodology that we had developed prior to the applicability of the GDPR [3, 18]. In a project funded by the German Ministry of Research and Education we then tested and refined this methodology. More specifically, we carried out a number of DPIAs in cooperation with companies and authorities using our methodology. This paper gives an insight into the experiences we had and the conclusions that can be drawn from them.

The rest of this paper is organized as follows: Sect. 2 briefly discusses some of the existing DPIA frameworks, their merits and shortcomings, then Sect. 3 outlines the methodology that we sought to validate. Sections 4 and 5 present and discuss the results from the empirical work. Section 6 concludes the paper.

## 2 Related Work

As the GDPR itself does not specify any specific operationalization for data protection impact assessments, stakeholders from different backgrounds have proposed approaches to fill this gap. Most of these methods are in principle suitable for fulfilling the requirements of Art. 35 GDPR [29, 38]. The most important approaches come from data protection authorities. These are attractive for the data controllers because they are officially rubber-stamped.

The most popular methodological framework was developed by the *French Data Protection Authority CNIL* [10] based on the EBIOS risk management

methodology of the French national IT security authority ANSSI.<sup>1</sup> In this approach, the assessment comprises of a highly structured and detailed but “checklist”-style query system that closely follows the legal text and inquires as to typical technical implementations – supported by a software tool. In this process, stakeholder consultation is not at the centre of the assessment. Rather, the input for the necessary analyses (on risk, proportionality, etc.) comes from the controller. The views of the data subjects are sought for the purpose of validating the results at the end of the process. In general, the CNIL operationalizes the DPIA as a compliance check of the GDPR and IT security requirements. Many other institutions, e.g. the German Association for Information Technology, Telecommunications and New Media BITKOM [17], have followed the CNIL in this approach.

The other influential DPIA framework was developed by the *Information Commissioner’s Office ICO* in the United Kingdom [23] and adapted by other national DPAs [1]. In particular, this framework builds on the long-standing tradition of privacy impact assessments (PIAs), which have been used in the English-speaking world since the 1990s [7, 40]. The most important offspring of the ICO approach is the ISO/IEC 29134 standard [25] – although this was adopted before the GDPR came into force and is therefore not fully compliant, ISO standards have a unifying effect and are readily used by (especially internationally operating) companies.

The ICO (and ISO) take a more reflexive and discursive approach, producing continuous text and asking more qualitative - and even organisational-sociological - questions (e.g. how to avoid “function creep”, the creeping expansion of processing purposes). Such an approach is more flexible in addressing the characteristics of very different applications, but the results tend to be less precise and verifiable. Instead of a relatively static request for specific implementations and guarantees, there is a more discursive, often workshop-based development of damage scenarios. For this reason, consultation of data subjects has a much greater importance in all steps of the process. The biggest weakness, in our view, is that the principles in Art. 5 GDPR are not further operationalized. This means that, for example, difficult legal concepts such as lawfulness, fairness and appropriateness, which are usually unfamiliar to legal laypersons, have to be discussed with data subjects or other stakeholders.

This weakness was recognised by the German supervisory authorities which proposed a so-called standard data protection model (SDM) [11]. The SDM is a general concept relevant for the GDPR as a whole, rather than a DPIA framework in the strict sense. However, it contains important elements that can be used for the purpose of creating a framework for operationalizing the DPIA requirement. In particular, the SDM uses the concept of protection goals, developed by Rost, Pfitzmann and others [34], and places them - instead of the data protection principles from Art. 5 GDPR – at the centre of operationalization. Of course, the protection goals do not contradict the principles of Art. 5 GDPR.

---

<sup>1</sup> <https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/> (last accessed 25-07-2021).

On the contrary, as has been shown in [11], the protection goals completely cover the principles of Art. 5. However, they translate the principles into the language of IT-Security (from where the concept of “protection goals” was originally taken), presenting the principles in a concise and condensed form. The authors of this paper have developed their own DPIA framework based on their own preliminary work [3] using the SDM protection goals. The goal of our methodology is a process that effectively identifies relevant data protection risks in a participatory manner. In the following sections, we analyse our experience with this process and what needs to be considered in order to carry out a DPIA across a heterogeneous group of stakeholders.

Since services are of increasing complexity, controllers need detailed information about a service to carry out a DPIA. Therefore the DPIA methodology proposed by the Government of the Netherlands [31] contains a so-called umbrella DPIA where service providers implement a general DPIA, which can then be used as a basis for individual risk assessments based on a specific context. An example of such a generic DPIA is the DPIA for diagnostic data processing in Microsoft Windows 10 Enterprise [30].

Thus, although there is a plethora of available DPIA methods, there has not been much work to evaluate and compare them from a *practical* perspective, e.g. [38]. There are two main types of studies: Evaluations of approaches to implementing DPIA or sub-elements thereof [14, 29] and studies on the notion of risk under the GDPR [15, 19, 21].

Finally, there are a number of publications presenting DPIA results for critical technologies such as facial recognition [6], COVID-19 contact tracing apps [5] or eHealth [26, 35] that also report implementation experiences selectively [4].

### 3 Operationalization of DPIA<sup>2</sup>

The operationalization of the DPIA methodology presented below is structured as described in Table 1, where the central DPIA consists of the *DPIA preparation*, *execution* and *DPIA implementation* accompanied by the *initialization* and *sustainability* phase. An important aspect of a DPIA is responsibility. In general, the controller of data processing is responsible for performing a DPIA (Art. 35 (1) GDPR), potentially assisted by processors (Art. 28 (3)(f) GDPR). In addition the controller should seek the advice of the data protection officer (Art. 35 (2) GDPR). Participation of data subjects or their representatives is in general recommendable. Especially in relation to complex services, advice from processors or even technology providers may be helpful. During the case study, workshops with organizations in different roles, i.e. controller, processor or technology provider, were performed.

---

<sup>2</sup> A detailed description of the methodology can be found in [28].

**Table 1.** Overview of DPIA phases [28, p. 24]

DPIA phase	Description
I. Initiation phase	– Threshold assessment: Clarify whether a DPIA is necessary
II. Preparation phase	– Description of the processing operations & collection of information, – Planning of the execution phase
III. Execution phase	– Consultation of the data subject (or their representatives) – Risk identification and analysis – Risk assessment, mitigation measures, assessment of remaining risks – Assessment of the necessity and proportionality <i>In case of high remaining risks → consult with the supervisory authorities or abandon the processing</i>
IV. Implementation phase	– Implementation of the mitigation measures – Test of the mitigation measures (where possible before the start of the processing) – Proof of compliance with the GDPR <i>→ Processing can go ahead</i>
V. Sustainability phase	– Monitoring – Identification of deviations or changes – Adjustments <i>Depending on the size of deviations or changes → potentially repeat phases II. to IV.</i>

### 3.1 Initialization Phase

In the first phase, the *initialization phase* the aim is to analyze whether a DPIA is necessary for a processing activity. The so-called “threshold analysis” is itself a first rudimentary risk assessment based on a few criteria, which – like the full DPIA – must be carried out before the processing of personal data starts. The records of processing activities (Art. 30(1) GDPR), the documentation of lawfulness (Art. 6 GDPR) and preliminary considerations of necessity and adequacy (Art. 5 GDPR) could serve as a basis for this initial step.

In this phase, the controller is obliged to consider whether the processing is likely to result in a high risk to the rights and freedoms of natural persons according to Art. 35 (1) GDPR. Besides the indications concerning processing activities in Art. 35 (3) GDPR, supervisory authorities should establish and communicate lists of processing activities which fulfill the relevant criteria (Art. 35 (4) and Art. 68 GDPR). In addition, the criteria of the Article 29 Data Protection Working Party should be considered [2]. The result of this threshold analysis should be documented.

In the context of the case studies, this initialization phase was conducted via preliminary communication with the organizations. In these preparatory

**Table 2.** Description of the processing operations and collection of information

Aspect	Summary of preparation
Data subjects	<ul style="list-style-type: none"> <li>– Data subjects</li> <li>– Representatives (e.g. work council)</li> </ul>
Organization	<ul style="list-style-type: none"> <li>– Controllers</li> <li>– Processors resp. joint controllers</li> <li>– Other stakeholders in general</li> <li>– Description of organizational structure</li> </ul>
Data processing	<ul style="list-style-type: none"> <li>– Description of personal data</li> <li>– Documentation of data flows (e.g. in the form of a data flow diagram)</li> <li>– (Intended) processes as context for data processing</li> </ul>
Technical documentation	<ul style="list-style-type: none"> <li>– Documentation of the (intended) technical implementation</li> <li>– Technical infrastructure</li> <li>– Existing or planned technical and organizational measures</li> </ul>
Legal documents	<ul style="list-style-type: none"> <li>– Contracts</li> <li>– Work council agreements, etc.</li> </ul>

conversations, other relevant issues such as information gathering on processing operations were also discussed.

### 3.2 DPIA Preparation Phase

If during the initialization phase potentially high risks for the rights and freedoms of natural persons are detected, a full DPIA needs to be carried out.

The first step in the *DPIA preparation phase* according to Art. 35 (7)(a) GDPR is “a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller”. In addition to the records of processing activities, toward this end, information about the intended processing activities and the context of processing should be provided to facilitate the privacy risk assessment in the subsequent *DPIA execution phase* (see Table 2).

In addition the *DPIA execution phase* needs to be planned and a proposal for an adequate team assisting the controller performing the DPIA is needed.

An important aspect of this phase is the detection of all persons involved in, and affected by, the processing activities. Especially via the use of workflow management systems and meta data in general, customer data and the personal data of staff members is often collected - the latter potentially allowing performance control of work processes. In the case of IoT services such as smart homes, smart mobility services or even CCTV applications, beside the intended users, the personal data of friends, family members, employees, etc. may also

be processed. For complex products or services which are part of the intended processing, details of processing are typically not completely documented and service providers, technology providers, human resources representatives, process experts or IT experts are helpful for clarifying details. An important tool is a data flow diagram to detect all stakeholders and interfaces with data transfers.

### 3.3 DPIA Execution Phase

The focus of the execution phase is the assessment of risks to the rights and freedoms of data subjects<sup>3</sup> (Art. 35 (7)(c) GDPR), the choice of measures to address the risks and to ensure the protection of personal data (Art. 35 (7)(d) GDPR) and the assessment of the necessity and proportionality of the processing operations in relation to the purposes (Art. 35 (7)(b) GDPR).

Based on the information collected in the *DPIA preparation phase* the DPIA team conducts the risk identification and analysis for risk assessment. At the start of the process, a common understanding of the intended processing is developed.

**Risk Identification.** The first goal is the identification of privacy risks. In the context of our case study an approach adapted from scenario analysis was used [24]. Based on the information about data subjects and personal data processed, scenarios incorporating potential harms to data subjects are identified via brainstorming. For these scenarios the information summarized in Table 3 is collected concerning the identified scenario in question (*damage scenario*). In addition, information about technical and organizational measures which are already present in the processing operation should be collected in parallel (*existing countermeasures*) as, typically, new processing activities are realized in the context of an existing IT landscape which employs standard security and privacy measures.

**Risk Analysis.** The next step is to analyze the identified risks from the viewpoint of the data subject. Instead of the abstract normative provisions in the GDPR, our methodology uses the data protection goals defined in the SDM as an assessment benchmark [11]. They are more suited to practical work because they translate the abstract norms into concrete system requirements. These are much better understood by people involved in a DPIA as they allow to establish a direct link to the functionality and implementation of the data processing to be assessed. The protection goals include:

- *Data Minimisation* stands for the principle of necessity, according to which no more personal data are to be processed than are needed to achieve the purpose.

---

<sup>3</sup> This means that not only the risks to the right to data protection (Art. 8 CFR) and the right to respect for private and family life (Art. 7 CFR) have to be considered, but also the other fundamental rights in the Charter [21]. In our test cases however, the focus was on data protection risks.

**Table 3.** Documentation of risk assessment

Aspect	Description
Damage scenarios	<ul style="list-style-type: none"> <li>– Description of the scenario</li> <li>– Data subjects</li> <li>– Personal data</li> <li>– Involved actors/stakeholders</li> <li>– Potential harm/damage for data subjects</li> <li>– Elements triggering the harm/damage</li> </ul>
Existing countermeasures	– Already existing technical and organizational mitigation measures
Data protection goals	<p><i>Describe how data protection goals are affected and prioritize the goals together with data subjects resp. representatives</i></p> <ul style="list-style-type: none"> <li>– Data Minimisation</li> <li>– Availability</li> <li>– Integrity</li> <li>– Confidentiality</li> <li>– Unlinkability</li> <li>– Transparency</li> <li>– Intervenability</li> </ul>
Risk assessment	<ul style="list-style-type: none"> <li>– Severity of the potential damage (minor, manageable, substantial, major)</li> <li>– Likelihood (minor, manageable, substantial, major)</li> <li>– Resulting Risk Level (low risk, normal risk, high risk)</li> </ul>
Additional measures	<p><i>Also processing activities might be changed resulting in an adapted risk assessment</i></p> <ul style="list-style-type: none"> <li>– Additional mitigation measures</li> <li>– Enhancement of existing measures</li> </ul>

- *Availability* refers to the requirement that personal data must be available and can be used properly in the intended process.
- *Integrity* stands for the requirement (a) that IT processes and systems continuously comply with specifications and (b) that the data to be processed remain intact, complete, and up-to-date.
- *Confidentiality* means that no person is allowed to access personal data without authorisation.
- *Unlinkability* is the requirement that data shall be processed and analysed only for the purpose for which they were collected.
- *Transparency* means that the data subject, system operators, and supervisory authorities must be able to understand the how and why of any data processing.
- *Intervenability* refers to the requirement that data subjects can actually exercise their rights of notification, access, rectification, blocking and erasure at any time.



Just as there are usually tensions between the interests of different stakeholders, the protection goals are not independent but influence each other. This means that not all protection goals can be fulfilled to the same extent. If complete confidentiality is guaranteed in a system, this means that access to certain data is restricted for certain actors, i.e. availability is limited. There is also a trade-off between integrity and intervenability, because integrity means that subsequent changes to data and processes are not allowed, while intervenability means that changes are allowed e.g. in the form of the right to rectification. Finally, there is also a conflict between transparency and unlinkability, as the former aims to increase the understanding of the actual data processing, e.g. by logging the actions of users and administrators, whilst the latter tries to avoid creation of such surplus knowledge [22,39].

During the workshops the protection goals were well understood and helpful for participants describing their privacy perception and priorities in the context of a concrete scenario. When carrying out the assessment, consideration should also be given to which protection goals are most important to the data subjects and other stakeholders concerned in the context of the scenario. This can and will lead to a prioritisation of the protection goals in relation to each scenario.

**Risk Assessment.** After the analysis of risks, the likelihood of the occurrence of risks and the severity of consequent harm are estimated by the DPIA team. This is typically done from the subjective viewpoint of the data subjects on a scale ranging from *minor*, *normal*, *substantial*, *major*: 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. 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.

The value of such a procedure leading to a purely qualitative classification lies in the fact that in the discourse either a consensual assessment is reached or a potential conflict is revealed. Both outcomes are useful for risk mitigation.

The result of the risk evaluation can be visualized in a risk matrix in order to gain an overview of existing privacy risks. There risks are roughly quantified as *low*, *normal* or *high*. In the context of a continuous improvement process,

necessary additional, or adapted, technical and organizational measures are defined and/or the processing activities themselves are changed to reduce risks to the rights and freedoms of natural persons. The aim is to ensure the protection of personal data and to demonstrate compliance (Art. 35 (7)(d) GDPR). In addition, an assessment of the necessity and proportionality of the processing operations in relation to the purposes of processing is performed (Art. 35 (7)(b) GDPR).

The whole process, including information collected in the DPIA preparation phase, the result of the risk assessment and the measures defined to address risks, must be documented in a comprehensive DPIA report (Art. 35 (7) GDPR).

If the risks can be reduced to an acceptable extent - such that the intended processing is compliant with the GDPR - the processing can be implemented incorporating the defined measures. Otherwise, a prior consultation of the supervising authority is needed: the intended processing may have to be abandoned if the risks cannot be eliminated or at least reduced to an acceptable extent.

### 3.4 DPIA Implementation Phase

In this phase the measures defined in the DPIA report are implemented and the effectiveness of measures is tested and documented to the extent possible before the approval of GDPR compliance. For the monitoring of risks and effectiveness of defined measures, a monitoring and test concept has to be developed and implemented, including a comprehensive documentation of test results. It is advisable to integrate this monitoring into a data protection management system, which is ideally part of the organisation's risk management approach. After ensuring the compliance of processing activities with the GDPR, the processing can begin.

### 3.5 Sustainability Phase

During the operation of a system, the controller must continuously ensure that, in the context of the processing, the risks to the rights and freedoms of natural persons are adequately reduced. Therefore, risks and effectiveness of implemented measures have to be monitored based on the defined test concept.






In case of slight deviations to the envisaged processing, the risk assessment, the measures and the DPIA, can all be adjusted. If significant changes or operational differences occur, the controller needs to adapt phases II. to IV. in Table 1.

## 4 Methodology of the Case Studies

In 2018/19, we worked with twelve organisations (corporate and public) in conducting DPIAs using the methodology presented in Sect. 3. We have analysed real data processing operations as used by the partner organisations in their daily business.

The aim was to operationalize, test and adapt an earlier version of the presented DPIA approach [18] on the basis on the experience gained in these validation tests. In particular, we wanted to find out whether the framework works equally well in organisations of different sizes and from different sectors, or whether significant differences might exist. The sample of organisations (Table 4) finally included 3 start-ups or micro-enterprises, 2 SMEs, 5 large companies and 2 public administrations (cities). These came from different economic sectors and included for-profit and non-profit organisations. Although most technology providers are not obliged to carry out a DPIA under the GDPR, there is strong demand on the part of their clients for input and/or for collaboration. For this reason, we also conducted a validation workshop with an automotive supplier.<sup>4</sup>

**Table 4.** Number, role and sector of test candidates

	Controller	Processor	Technology Provider
Mobility 		1	1
Health 	3	2	
Telecommunications 		1	
Public authority 	2		
Retail 	2		

The focus of the case studies was mainly on phases II. and III. of our framework and in particular on risk identification, analysis and assessment. The workshops lasted typically one full day per organization and were mainly composed of the following elements:

- Workshop preparation
  1. Decision about the processing activity to be considered in the workshop
  2. Collecting information about the processing activity based on a questionnaire/list of required information for the *DPIA preparation phase*.
- Workshop
  3. Finalization of the *DPIA preparation phase* in the first part of the workshop
  4. Privacy risk assessment of the *DPIA execution phase* in the second part of the workshop for selected risks.
  5. Final discussion and feedback

<sup>4</sup> It was interesting to note that organisations are often not aware that there might be joint controllership with a service or software provider and that these then also have to contribute to the DPIA.

The composition of the group of participants was quite diverse - and was varied as an element of the study concept. In all cases the data protection officer (or the responsible manager) was present. In addition, in most cases, representatives from IT (security) and people responsible for the processing were also involved. During workshops with startups, all members of the company usually took part as formal roles had often not been fully defined. In some workshops, especially in the retail and healthcare sector, employee representatives, and even data subjects or their representatives, were involved. In one workshop, representatives from (external) processors were also present because of the complexity of the service. Thus typically there was a mix of qualifications: the DPO in most cases has a legal and/or technical background, while the background of most others involved was not legal. Nevertheless, they were all experts in their field and needed to be taken seriously with regard to their professional principles and experiences.

Involving data subjects is a particular challenge, as they are usually not experts in any of the processing-related areas. However, they must be enabled to make an informed and sound assessment of the potential risks from their perspective. It is crucial that the person facilitating such a workshop does justice to all these aspects so as not to marginalise any viewpoint. This is a risk, especially in larger organisations that have already professionalised data protection. While they usually have sufficient knowledge about the provisions of the General Data Protection Regulation (GDPR), there is a tendency to focus on formal legal aspects (e.g. the existence of a legal basis for data processing), which is rather secondary to the risk perception of data subjects and other stakeholders.

For the evaluation of the workshops, there were two different roles in the study team. The first role was that of the auditor, who had to conduct the DPIA workshops as realistically as possible according to the methodology to be tested. The second role was that of the observer, who checked how the workshop participants responded to the auditor's questions, whether they were able to use the protection goals for the assessment and what kind of interaction took place between the workshop participants. For the evaluation of the workshop, the perceptions of the auditor(s) and the observer(s) were compared and changes were made in the workshop design. Such changes concerned, for example, the way the protection goals were presented or the order of the questions. The use of damage scenarios was also a result of this evaluation, as it became clear that a risk assessment is easier based on a tangible case than on an abstract description. Fortunately, no fundamental changes had to be made to the approach, so the methodology presented in Sect. 3 was basically confirmed.

## 5 Experiences from the Case Study

In the course of our validation tests, we have been able to gather a wide range of experience, (a) as to how prepared companies are to carry out DPIAs, (b) as to how understandable the assessment criteria are to stakeholders, and (c) how best to engage different stakeholders in the assessment process. Many of

these experiences have already been taken into account in the process outlined in Sect. 3. In the following, however, we will highlight and discuss the most important findings from the different process phases.

## 5.1 General Aspects

During the interviews and workshops it was pointed out that processors of personal data, and even technology providers who only provide technologies without any additional service, are sensitized to the obligation of DPIAs. Customers of processors, and even technology providers, now demand information about the privacy risks of services and information about technical and organizational measures deployed in relation to services. In most of the tests, besides focusing on the DPIA itself, the test candidates also used the workshops for discussions and exchange of experiences concerning general aspects of data protection within the organization.

## 5.2 In the Initialization Phase

In recent years, there has been intense debate in the scientific community about when data processing is “is likely to result in a high risk to the rights and freedoms of natural persons” [13, 19]. For practitioners this question is of little importance in the initialization phase. Rather, we experienced lively discussion in our workshops as to whether a DPIA was actually necessary for the selected processing. As there was a general fear of compliance violations and the corresponding fines, organisations tried to include a broad range of processing activities as requiring a DPIA to be on “the safe side”. In such a situation, it was helpful in providing guidance, especially to those organizations that had hitherto given little attention to data protection issues, that the data protection authorities have compiled authoritative lists of processing operations which are always subject to the requirement to undertake a DPIA (aka “blacklists”).

## 5.3 In the DPIA Preparation Phase

The actual *collection of information* in the DPIA preparation phase has not only shown the importance of a thorough analysis from the data subjects’ perspective, but also how incomplete the knowledge of those in charge of the DPIA is about the details and context of the processing to be assessed. On the one hand risks are overlooked which emerge from scenarios beyond normal processing activities: the (rare) cases in which law enforcement and supervisory authorities gain access to data are also often not problematized. On the other hand, there is often still a lack of awareness that the greatest risks usually come from processing for the intended purposes and by authorised actors [16, 33]. Instead, the focus is often on the malicious external attacker (aka “hacker”).

Due to the increasing *complexity and modularisation of IT services* and the incorporation of cloud services and IT providers in general, it was an intricate

task for many controllers to obtain the requisite information and understanding of their own processing activities. The involvement of processors is generally of utmost importance. It was promising that one SME which provided cloud services for companies as a processor demonstrated thorough data protection competencies and stated that data protection is a key selling point in its market. In the case of standard cloud services by international companies this would be difficult to realize. Another issue is the inherent agility of cloud services which are steadily changing. This is not always transparent to users. In this context compositional approaches towards DPIAs [36, 37] and generalized DPIAs for services [30] should be further investigated.

As a thorough basis for assessing data protection risks, it is of utmost importance to involve not only the controller, IT security experts, and data protection experts, but also individuals with in-depth knowledge of domain-specific workflows and processing activities and their technical implementation. It is advisable to involve additional stakeholders or their representatives. This *heterogeneity of the working group* must be taken into account by a transparent methodological approach. In the first round of testing, we worked with interviews structured along the protection goals. In the interview-based workshops it turned out that, for people without deep knowledge in privacy and data protection, the privacy risks for data subjects in the context was not sufficiently clear. It proved more useful to carry out the assessment in a participatory way based on collaborative identification and analysis of scenarios (see Table 3) which might cause damage to data subjects.

One implication that emerged from the case studies was that concrete risks to data subjects were often a function of complex and highly domain- and use case-specific details of the particular processing activities. Domain/use case experts with deep knowledge of the details and context of the particular processing activity – but often limited knowledge of data protection – frequently provided crucial insights here, based on their deep “everyday knowledge” of the processing and its context. This suggests that one risk for conducting good DPIAs is excessively foregrounding the expertise and authority of data protection lawyers and professionals (who will usually have limited understanding of the use-case details and context), and downplaying the inputs and expertise of the domain professionals.

#### 5.4 In the DPIA Execution Phase

The *choice of words* in the risk assessment in particular is very important for participants. In particular, terms with negative connotations from IT security – such as “attacker” or “source of risk” – almost lead to the exclusion of internal stakeholders in the following discussion. In their self-image, they do not perceive themselves as a “risk factor”. In this regard it is necessary to meet them on the level of their core expertise. Choosing negative wording could potentially cause harm in scenarios where the purpose of the processing is only slightly extended and the parties involved act with the best intentions, i.e., do not intend to cause any harm. Thus more neutral terms such as “stakeholders”, “triggers for the scenario” etc. are used to facilitate the brainstorming. Since IT security risks

caused by external attackers have already been sufficiently considered in most cases, we have focused on scenarios triggered by internal actors.

Apart from internal attackers, internal data subjects such as employees were also not always in focus for the DPIA teams in the workshops. Often, privacy risks were mainly identified and analyzed from the point of view of external data subjects as customers, users or patients. *Risks for internal data subjects*, i.e. employees were considered as of lower priority. When employees such as data subjects are present, it is important to consider power inequalities in the DPIA team. Hence, it is advisable to incorporate work council members. Also, data subjects which are not directly customers, users or patients - e.g. friends and family - were often overlooked. Therefore, we mainly concentrated on these types of data subjects. It is important in DPIA execution to raise awareness concerning these data subjects.

For stakeholders who are involved as data subjects and who are not data protection experts, the concept of privacy is rather vague and is often misunderstood as restricted to confidentiality. We perceived during the workshops that the data protection goals allowed these stakeholders to formulate their personal privacy perceptions and priorities. Here, context is particularly important. For example, in the health care sector, availability and integrity of documented work processes and activities may be much more important to employees than confidentiality, whereas in HR data management, confidentiality and unlinkability are paramount. In other cases transparency and intervenability were stated as the most important goals. The fact that the protection goals are explicitly framed (and often graphically presented) as countervailing principles that partially stand in tension to each other and can require balancing trade-offs proved particularly helpful in this case, as it seemed to give stakeholders (especially those without legal expertise) greater confidence to state which risks and protection goals in the particular use case were of paramount importance to them, and where tradeoffs to secure these were acceptable.

During the workshops in the *DPIA execution phase*, many participants asked for guidance through *checklists and risk catalogs*. Although the desire for checklists is understandable and their use has a practical value, the implementation of a DPIA must not become a purely mechanical checklist work-through exercise. Because the focus of a DPIA is to identify privacy risks in specific contexts where innovative technologies, etc. are used, it is important to explore risks beyond standardized lists. However, it may be useful to provide participants with illustrative examples to give them an idea of what is understood as risk for the purposes of the DPIA. In particular, it turns out that a small number of typical risks - largely independent of the application domain - occur again and again. These can be reused when similar processing activities in similar contexts are investigated and allow a transfer of results from DPIAs to the standard risk-based approach. Some examples that can serve as illustrations are provided in [9, 18].

Stakeholders with an IT security background, in particular, questioned several times why, in our methodology, risks were assessed with a *qualitative risk assessment instead of quantitative approaches* as usually employed for security

risks. It was important to point out that several privacy related risks are so-called “chilling effects” which always occur - e.g. people feel surveyed because of the existence of CCTV and therefore feel restricted with regard to exercising their right to protest [16,32]. In addition, in most cases it is not possible to state the cost of such an incident for the individual.

## 5.5 In the DPIA Implementation Phase

During our workshops we concentrated on the initiation, DPIA preparation and DPIA execution phases. But it was obvious that identifying and assessing the severity of a risk alone was not enough. For many controllers, the immediate question arose as to how a risk could best be addressed. At this point, well-maintained catalogs of reference measures are of great benefit. Fortunately, such catalogs have already been created by national supervisory authorities such as the CNIL [9] or the German Data Protection Conference.<sup>5</sup>

## 5.6 In the Sustainability Phase

An important point of discussion during the workshops was the question of how DPIAs can be updated on a regular basis. To this end, it would make sense to integrate DPIAs into the standard risk assessment and risk management processes of organizations, as suggested in [8,17,41].<sup>6</sup>

## 6 Conclusions

According to first experiences with DPIAs (and many years of experience with privacy impact assessments), it can be stated that DPIA is basically a good instrument to support decision-makers and developers, if it is not merely regarded as a compulsory exercise, but as a useful tool. The systematic identification of risks is a valuable basis for strategic action by implicated actors for the continuous improvement of products and services. It also provides an opportunity to evaluate potentially controversial data processing systems in relation to which a societal consensus is needed as to which risks should be acceptable and which should not. DPIA results can provide the basis for this.

But the potential of DPIAs will not unfold automatically. A broad and effective consultation of stakeholders and data subjects requires a relatively high level of time, organizational and material effort. The DPIA process developed as part of our work, and the methods and tools used to engage individuals from diverse backgrounds, are promising, but also made clear that additional issues need to be addressed:

<sup>5</sup> <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/> (last accessed 30-07-2021).

<sup>6</sup> We have (anecdotal) evidence that this is a challenging task, as it requires a comprehensive modelling of the system landscape and data flows that does not exist in most organizations. Therefore, the solutions we know are either trivial or highly complex.



Any specialist knowledge required (in particular technical or legal) must be communicated to the participants in such a way that it can be understood by laypersons. In this context, attention must be paid to the effect of different formulations, which may unintentionally favor technophile participants or those with legal knowledge, for example. This is important not only from a normative point of view, but also from a practical perspective: it makes little sense to conduct a focus group, for example, without ensuring that all group members can also contribute.

Communication processes both among the participants, and between them and the organization, must be designed in such a way that communication barriers are reduced, misunderstandings are avoided, and, as far as possible, everyone can participate to the same extent. Furthermore it has to be taken into account that some of the participants in the DPIA can be the source of a data protection risk and the affected data subjects at the same time. Finally most participants are employees of an organisation or company and therefore have to act in accordance with what is in the best interests of the business. This can lead to tensions when they are supposed to assess risks in an unbiased way from the point of view of the people concerned. Again, this is both a functional and a practical imperative: stakeholder consultations dominated by a few participants are rarely appropriate. Here, the use of external facilitators with experience in consultation processes can be helpful.

Finally, it should not go unmentioned that a DPIA (like any formalized procedure) also specifies what must remain outside the scope of the assessment. For this reason, scientifically oriented DPIAs are useful, for example, for the area of research and development, even if they do not necessarily meet the requirements of the GDPR for a DPIA. They do, however, make it possible to integrate data protection issues into the risk management of technology producers and system operators. This can provide a balance, often missed in technology assessment, between the desire for normativity on the one hand and operationalization on the other [20].

**Acknowledgement.** This work was partially funded by the German Ministry of Education and Research under grant nos. 03VP03551, 03VP03553 and 16KIS0741K. Our thanks to Britta Mester (Datenschutz Nord GmbH) and Meiko Jensen (Kiel University of Applied Research) who contributed to the work presented in this paper.

## References

1. Agencia Española de Protección de Datos (AEPD), Madrid: Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD (2018). <https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf>
2. Article 29 Data Protection Working Party, Brussels: Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (2017). [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=47711](http://ec.europa.eu/newsroom/document.cfm?doc_id=47711)

3. Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M.: A process for data protection impact assessment under the European general data protection regulation. In: Schiffner, S., Serna, J., Ikonomidou, D., Rannenberg, K. (eds.) APF 2016. LNCS, vol. 9857, pp. 21–37. Springer, Cham (2016). [https://doi.org/10.1007/978-3-319-44760-5\\_2](https://doi.org/10.1007/978-3-319-44760-5_2)
4. Bisztray, T., Gruschka, N.: Privacy impact assessment: comparing methodologies with a focus on practicality. In: Askarov, A., Hansen, R.R., Rafnsson, W. (eds.) NordSec 2019. LNCS, vol. 11875, pp. 3–19. Springer, Cham (2019). [https://doi.org/10.1007/978-3-030-35055-0\\_1](https://doi.org/10.1007/978-3-030-35055-0_1)
5. Bock, K., Kühne, C.R., Mühlhoff, R., Ost, M.R., Pohle, J., Rehak, R.: Data protection impact assessment for the corona app. <https://doi.org/10.2139/ssrn.3588172>
6. Castelluccia, C., Le Métayer, D.: Position paper: analyzing the impacts of facial recognition. In: Antunes, L., Naldi, M., Italiano, G.F., Rannenberg, K., Drogkaris, P. (eds.) APF 2020. LNCS, vol. 12121, pp. 43–57. Springer, Cham (2020). [https://doi.org/10.1007/978-3-030-55196-4\\_3](https://doi.org/10.1007/978-3-030-55196-4_3)
7. Clarke, R.: Privacy impact assessment: its origins and development. *Comput. Law Secur. Rev.* **25**(2), 123–135 (2009). <https://doi.org/10.1016/j.clsr.2009.02.002>
8. Coles, J., Faily, S., Ki-Aries, D.: Tool-supporting data protection impact assessments with CAIRIS. In: 2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPREE), pp. 21–27. IEEE Computer Society, Los Alamitos, August 2018. <https://doi.org/10.1109/ESPREE.2018.00010>
9. Commission Nationale de l'Informatique et des Libertés (CNIL), Paris: Privacy Risk Assessment: Knowledge Bases (2018). <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>
10. Commission Nationale de l'Informatique et des Libertés (CNIL), Paris: Privacy Risk Assessment: Methodology (2018). <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>
11. Conference of the independent data protection authorities of the Federal and State Governments of Germany: The Standard Data Protection Model: A method for data protection advising and controlling on the basis of uniform protection goals (2020). [https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology\\_V2.0b.pdf](https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf)
12. De, S.J., Le Métayer, D.: Privacy Risks Analysis. Morgan & Claypool (2016). <https://doi.org/10.2200/S00724ED1V01Y201607SPT017>
13. Demetzou, K.: Data protection impact assessment: a tool for accountability and the unclarified concept of 'high risk' in the general data protection regulation. *Comput. Law Secur. Rev.* **35**(6), 105342 (2019). <https://doi.org/10.1016/j.clsr.2019.105342>
14. Demetzou, K.: Processing operations 'likely to result in a high risk to the rights and freedoms of natural persons': lessons to be learned from national authorities' DPIA 'blacklists'. In: Antunes, L., Naldi, M., Italiano, G.F., Rannenberg, K., Drogkaris, P. (eds.) APF 2020. LNCS, vol. 12121, pp. 25–42. Springer, Cham (2020). [https://doi.org/10.1007/978-3-030-55196-4\\_2](https://doi.org/10.1007/978-3-030-55196-4_2)
15. van Dijk, N., Gellert, R., Rommetveit, K.: A risk to a right: beyond data protection impact assessments? *Comput. Law Secur. Rev.* **32**(2), 286–306 (2016). <https://doi.org/10.1016/j.clsr.2015.12.017>
16. European Data Protection Supervisor, Brussels: Accountability on the Ground Part II: Data Protection Impact Assessments and Prior Consultation (2019). <https://edps.europa.eu/node/4582.env>
17. Federal Association for Information Technology, Telecommunications and New Media (BITKOM), Berlin: Risk Assessment & Data Protection Impact Assessment - Guide (2017). <https://www.bitkom.org/sites/default/files/file/import/170919-LF-Risk-Assessment-ENG-online-final.pdf>

18. Friedewald, M., et al.: Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz. Fraunhofer ISI, Karlsruhe (2017). <https://www.forum-privatheit.de/wp-content/uploads/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf>
19. Gellert, R.: Understanding the notion of risk in the General Data Protection Regulation. *Comput. Law Secur. Rev.* **34**(2), 279–288 (2018). <https://doi.org/10.1016/j.clsr.2017.12.003>
20. Grunwald, A.: Technology assessment or ethics of technology? Reflections on technology development between social sciences and philosophy. *Ethical Perspect.* **6**(2), 170–182 (1999). <https://doi.org/10.2143/EP.6.2.505355>
21. Hallinan, D., Martin, N.: Fundamental rights, the normative keystone of DPIA. *Eur. Data Prot. Law Rev.* **6**(2), 178–193 (2020). <https://doi.org/10.21552/edpl/2020/2/6>
22. Hansen, M., Jensen, M., Rost, M.: Protection goals for privacy engineering. In: SPW 2015: Proceedings of the 2015 IEEE Security and Privacy Workshops, pp. 159–166. IEEE, Washington (2015). <https://doi.org/10.1109/SPW.2015.13>
23. Information Commissioner’s Office (ICO), Wilmslow, UK: Guide to the General Data Protection Regulation (GDPR) (2021). <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf>
24. ISO/IEC 27001:2013(E): Information technology - Security techniques - Information security management systems - Requirements. International Standardisation Organisation, Geneva (2013)
25. ISO/IEC 29134:2017(E): Information technology - Security techniques - Guidelines for privacy impact assessment. International Standardisation Organisation, Geneva (2017)
26. Iwaya, L.H., Fischer-Hübner, S., Åhlfeldt, R.M., Martucci, L.A.: Mobile health systems for community-based primary care: identifying controls and mitigating privacy threats. *JMIR Mhealth Uhealth* **7**(3), e11642 (2019). <https://doi.org/10.2196/11642>
27. Kloza, D., et al.: Towards a method for data protection impact assessment: making sense of GDPR requirements. *d.pia.lab Policy Brief 1/2019*, VU Brussels, Brussels (2019). <https://doi.org/10.31228/osf.io/es8bm>
28. Martin, N., Friedewald, M., Schiering, I., Mester, B.A., Hallinan, D., Jensen, M.: The Data Protection Impact Assessment according to Article 35 GDPR: A Practitioner’s Manual. Fraunhofer Verlag, Stuttgart (2020). <http://publica.fraunhofer.de/dokumente/N-590015.html>
29. Martin, N., Schiering, I., Friedewald, M.: Methoden der Datenschutz-Folgenabschätzung: Welche Unterschiede bieten die verschiedenen methodischen Ansätze? *Datenschutz und Datensicherheit - DuD* **44**(3), 154–160 (2020). <https://doi.org/10.1007/s11623-020-1242-z>
30. Mas, S., Terra, F.: DPIA Office 365 ProPlus version 1905. Data protection impact assessment on the processing of diagnostic data. Ministry of Justice and Security, The Hague. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise/DPIA+Office+365+ProPlus+spring+2019+22+July+2019+public+version.pdf>
31. Ministerie van BZK, The Hague: Model gegevensbeschermings-effectbeoordeling rijksdienst (PIA). <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia.pdf>

32. Raab, C., et al.: Effects of surveillance on civil liberties and fundamental rights in Europe. In: Wright, D., Kreissl, R. (eds.) *Surveillance in Europe*, pp. 259–318. Routledge (2015). <https://doi.org/10.4324/9781315851365>
33. Rost, M.: Risiken im Datenschutz. *Vorgänge: Zeitschrift für Bürgerrechte und Gesellschaftspolitik* **57**(1/2), 79–91 (2018)
34. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele - revisited. *Datenschutz und Datensicherheit* **33**(6), 353–358 (2009). <https://doi.org/10.1007/s11623-009-0072-9>
35. Todde, M., Beltrame, M., Marceglia, S., Spagno, C.: Methodology and workflow to perform the data protection impact assessment in healthcare information systems. *Inform. Med. Unlocked* **19**, 100361 (2020). <https://doi.org/10.1016/j.imu.2020.100361>
36. Van Landuyt, D., Sion, L., Dewitte, P., Joosen, W.: The bigger picture: approaches to inter-organizational data protection impact assessment. In: Boureau, I., et al. (eds.) *ESORICS 2020*. LNCS, vol. 12580, pp. 283–293. Springer, Cham (2020). [https://doi.org/10.1007/978-3-030-66504-3\\_17](https://doi.org/10.1007/978-3-030-66504-3_17)
37. Vandercruysse, L., Buts, C., Doooms, M.: Practitioner’s corner: beyond data controllership: merits of a generic DPIA by hardware and technology suppliers. *Eur. Data Prot. Law Rev.* **6**(1), 133–136 (2020). <https://doi.org/10.21552/edpl/2020/1/18>
38. Vemou, K., Karyda, M.: An evaluation framework for privacy impact assessment methods. In: *12th Mediterranean Conference on Information Systems, MCIS 2018*, Corfu, Greece, 28–30 September 2018. AISEL (2018). <https://aisel.aisnet.org/mcis2018/5>
39. Wolf, G., Pfitzmann, A.: Properties of protection goals and their integration into a user interface. *Comput. Netw.* **32**(6), 685–700 (2000). [https://doi.org/10.1016/S1389-1286\(00\)00029-3](https://doi.org/10.1016/S1389-1286(00)00029-3)
40. Wright, D., De Hert, P. (eds.): *Privacy Impact Assessment*. Springer, Dordrecht (2012). <https://doi.org/10.1007/978-94-007-2543-0>
41. Wright, D., Wadhwa, K., Lagazio, M., Raab, C., Charikane, E.: Integrating privacy impact assessment in risk management. *Int. Data Priv. Law* **4**(2), 155–170 (2014). <https://doi.org/10.1093/idpl/ipu001>

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

