Illuminating the DPIA Blackbox – A Survey of Data Protection Impact Assessment Practices in Organisations

Malte Hansen[1(✉)], Greta Runge[2], Nils Gruschka[1], and Meiko Jensen[3]

[1] Department of Informatics, University of Oslo, Oslo, Norway
{maltehan,nilsgrus}@ifi.uio.no
[2] Fraunhofer Institute for Systems and Innovation Research, Berlin, Germany
greta.runge@isi.fraunhofer.de
[3] Karlstad University, Karlstad, Sweden
meiko.jensen@kau.se

Abstract. According to the European General Data Protection Regulation (GDPR), a Data Protection Impact Assessment (DPIA) is mandatory for all ongoing and planned processing of personal data if said processing is likely to affect the privacy and data protection rights and freedoms of the data subjects. However, upon examining the real-world implementation of this requirement, various approaches emerged, resulting in a heterogeneous landscape of DPIA processes.

In this paper, we present the results of a survey that investigated the state of adoption of DPIA process methodologies in real-world organisations. Our survey reveals that handwritten DPIA reports and ad-hoc methods continue to dominate the DPIA landscape in Europe. Moreover, according to our data, processes involving multiple stakeholders are often not adequately assessed in terms of DPIA-related risks.

Keywords: DPIA · data protection impact assessment · privacy impact assessment · GDPR

1 Introduction

New digital technologies are emerging at an increasing rate, and data processing is becoming increasingly important for their effectiveness. To manage resources for these processes, data sharing and the utilisation of external services, such as cloud services, are also expanding. This introduces various data protection risks that have to be addressed. An essential tool in assessing these challenges is a data protection impact assessment (DPIA), introduced as a mandatory requirement by the General Data Protection Regulation (GDPR) [1].

But how are DPIA processes implemented in practice? Published DPIA results are hard to find, and the available results are mostly limited to the DPIA report, which does not provide detailed insights into how the DPIA was

N. Arastouei et al. (Eds.): APF 2025, LNCS 16183, pp. 178–201, 2026.
https://doi.org/10.1007/978-3-032-07574-1_8

conducted. To gain information about the DPIA process itself, several guidelines, templates, and DPIA tools are available online. However, they are often very generic and do not adequately address an organisation's specific issues. This applies particularly to organisations engaged in data sharing or that are part of a large data ecosystem.

ENISA identified the risks stemming from the specific constellations of actors, such as unknowingly sharing sub-processors, in a data space as a major challenge [2]. The Big Data Value Association also recognised a lack of frameworks for addressing legal issues and proper risk evaluation in data sharing within data spaces [3]. Similarly, the Spanish supervisory authority AEPD stated that *"the DPIA and the solutions that manage the limitations and risks to rights and freedoms must emerge from a common effort"* [4, p. 69]. Recital 95 of the GDPR [1] further clarifies that processors should assist the controller during a DPIA. DPIA procedures, therefore, require special attention to address these challenges adequately. However, *"the task of supporting a holistic DPIA with multiple data controllers and data intermediaries is a non-trivial one"* [2, p. 13], and the aspect of a joint DPIA involving several different stakeholders with shared responsibility has not been explored yet by existing models [5]. This leads to the following research questions:

- **RQ1:** What are the current practices of the DPIA process in general?
- **RQ2:** What are the current challenges of the DPIA process?
- **RQ3:** How do current DPIA processes address external influences?

To answer these questions, we conducted an anonymous user survey asking about DPIA practices in organisations. The results of this survey are presented and discussed below in the following structure: We introduce the concept of DPIA in Sect. 2, followed by a review of related work in the field in Sect. 3. Afterwards, we introduce the methodology used for the survey in Sect. 4, followed by the presentation of the results in Sect. 5. The results are analysed and discussed in the context of different perspectives in Sect. 6 before summarising our findings and giving an outlook on future work in Sect. 7.

2 Background

The GDPR introduced DPIAs as a mandatory requirement for Data Controllers (DC) before implementing or updating IT systems and processes under certain conditions. To be precise, the GDPR states that a DPIA must be carried out *"where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons"* [1, Art. 35(1)]. To address these risks, a DPIA aims to cover the data flows and consequences of data processing as thoroughly as possible and to evaluate them objectively according to uniform criteria so that typical sources of risk can be countered with adequate technical and organisational measures. A short paper of the *Datenschutzkonferenz* of the German data protection authorities defines

the DPIA as *"a specific tool for describing, assessing and mitigating risks to the rights and freedoms of natural persons in relation to the processing of personal data"* [6, p. 1]. The French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), describes the DPIA as a tool for a DC to *"build and demonstrate the implementation of privacy protection principles so that data subjects retain control over their personal data"* [7, p. 4]. Furthermore, a DPIA aims to provide transparency to the public and policymakers, enabling an informed discussion about risks [8].

A key characteristic of the DPIA is its cyclic nature. The GDPR requires that the DPIA process be reviewed after a change to the risks of the processing (Art. 35(11), GDPR). The GDPR does not define an inherent methodology or process flow. However, researchers and data protection authorities have proposed various DPIA methodologies and models (see Sect. 3). A fundamental resource for these models is the guidelines on conducting a DPIA [9] released by the Article 29 Working Party, the predecessor of the European Data Protection Board (EDPB). These guidelines clarify basic principles, such as the execution threshold at which a DPIA becomes mandatory, also known as DPIA screening or threshold analysis, and the involvement of stakeholders. While they do not provide a methodology for these steps, they introduce a generic, iterative process for the execution of the DPIA following the threshold analysis, consisting of seven steps:

1. Description of the envisaged processing
2. Assessment of the necessity and proportionality
3. Measures already envisaged
4. Assessment of the risks to the rights and freedoms
5. Measures envisaged to address the risks
6. Documentation
7. Monitoring and review

Another approach to structuring the DPIA is to divide it into different phases. Martin et al. [10] structure the DPIA in five stages. Phase I, initiation of the DPIA, covers the threshold analysis. Next, the DPIA will be prepared in Phase II. This includes the process description, identification of Data Subjects (DSs) and stakeholders, and forming the DPIA team. Phase III describes the execution of the DPIA, beginning with the risk assessment and concluding with the documentation of the results in the DPIA report. Afterwards, Phase IV will implement the DPIA by testing the mitigation measures and demonstrating compliance, before the process enters the final Phase V, the periodic review of the DPIA.

While both approaches mostly follow the same procedure, they emphasise different steps. The procedure and overlap of the two approaches are illustrated in Fig. 1.

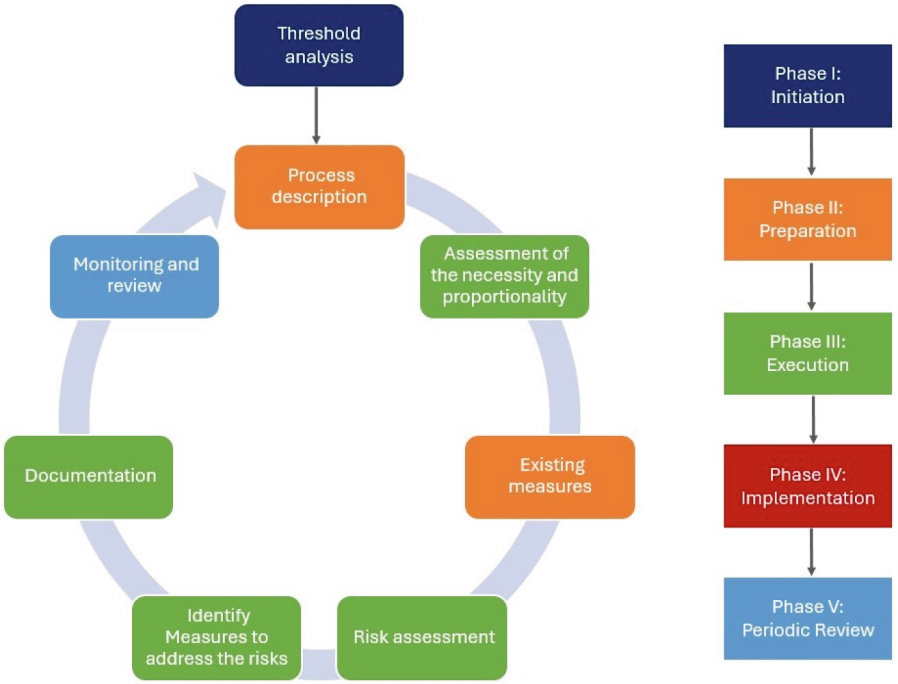

Fig. 1. Overlap of DPIA methodologies as defined by the EDPB/Article 29 Working Party [9] (left) and Martin et al. [10] (right)

3 Related Work

Following the introduction of the GDPR, various European data protection authorities, including the UK's Information Commissioner's Office (ICO) [11], the Spanish AEPD [12], and the French CNIL [13], developed text-based DPIA templates for quick adaptation by data controllers (DCs). Notably, CNIL also released a software tool and knowledge base [14], which explains essential notions of a DPIA to increase its ease of use. While not designed for DPIAs, the second version of the ISO/IEC 29134:2023 guidelines for privacy impact assessment [15] is a common reference.

In one of the first models for a DPIA, Bieker et al. introduced a three-phase process consisting of a *preparation*, *evaluation*, and *report and safeguards* stage [16]. A cornerstone of the evaluation stage in this approach is the identification of privacy protection goals, first introduced by Hansen et al. [17]. These protection goals expand the traditional information security goals of confidentiality, integrity, and availability with the privacy-focused goals of unlinkability, transparency, and intervenability. The privacy protection goals served as a fundamental resource in the approach introduced by Martin et al. [10] in Sect. 2 as well.

Later, Gonscherowski et al. did an exemplary execution of a DPIA in a mobility use case, utilising the principle introduced by Bieker et al. [18]. Haag et al. focused on explaining the process to medical staff, providing examples and a checklist while not including a concrete template [19]. An example of a template for a DPIA report can be found in the work of Kloza et al., which includes detailed input fields for legal, practical, and organisational considerations [20].

A review of common DPIA methodologies in practice by Nagele et al. highlights the improper application of DPIAs, lacklustre execution of the process, as well as a lack of common standards and guidelines [5]. Demetzou argues that the concept of 'high risk' is not legally qualified under the GDPR, leading to deficiencies during the threshold analysis [21]. A study assessing the implementation process of a DPIA in twelve companies further highlights the substantial resources required for a thorough DPIA. It identifies communication issues between technical, organisational, and legal professionals, as well as possible complications arising from an individual's role within the company [22]. A case study based on the approach by Martin et al. [10], running twelve tests in SMEs, acknowledges the potential of DPIAs as an instrument to support decision-makers and developers [22]. However, the tests also highlighted challenges in communication between DPIA team members, the resources required by the process, and potential conflicts with the business's interests. Further, a literature review by Wairimu et al. found that PIA methodologies, including DPIA methodologies, often lack evaluation and validation [23].

Georgiadis and Poels [24] conducted a literature review to develop a DPIA methodology tailored toward big data analytics. They conclude that, currently, no methodology exists that addresses all the requirements and privacy risks in the big data analytics sector. According to them, an ample list of provided privacy controls in a PIA process might be a bigger risk than an aid, highlighting the need for section-specific solutions [25]. This can also be seen in the differences in the methodology for healthcare information systems developed by Todde et al. [26], the guidelines for federated identity management models [27] and digital identity management in general [28], or the domain-specific refinements added to the LINDDUN privacy threat framework [29]. A different perspective on DPIAs is to see it as a tool to protect the interests of weak and underrepresented groups of individuals, for which current DPIA practices do not meet the norm [30].

As demonstrated by the approaches presented above, there is no uniform method for conducting a DPIA. While some small-scale case studies and insights into the DPIA procedures employed by organisations exist, an overview of best practices and common challenges with the DPIA process is hard to obtain.

The issue of a *compositional DPIA* involving data processing operations spanning multiple stakeholders has not been studied extensively. Horák et al. explored a DPIA for a cybersecurity data-sharing platform but have not looked at the joint execution of a DPIA. De and Le Métayer developed a privacy risk assessment methodology focusing on reusability [31]. A semantic specification for DPIAs by Pandit [32] is a crucial step towards creating machine-readable and shared DPIAs. However, the expression of principles and controls remains challenging.

Overall, existing DPIA approaches still lack several important properties required in collaborative processing scenarios: a formalised vocabulary to standardise results, means for accurate threshold analysis, a lack of reusability, procedures for risk assessment and measure selection, and means for multiple actors to work on the same DPIA process.

4 Methodology

As outlined in the research questions, this paper aims to gain a deeper understanding of organisations' current DPIA practices and the challenges they face, particularly regarding the federated constellations of actors within the regulatory European data ecosystem.

Section 3 highlights that there currently is no established standard process for DPIAs. Instead, various guidelines exist for both general and sector-specific use cases. Furthermore, these guidelines offer guidance and a sequence for the process, but do not provide detailed instructions on how to implement the components of the DPIA. As an internal process, there is no way to gain insight into these details except through the DPIA report, which is rarely made publicly available. The first step to understand the current state of DPIAs is therefore to learn about the general trends common in DPIA processes. For this reason, we conducted an anonymous, quantitative survey targeting professionals from diverse backgrounds who participated in a DPIA to learn about the structure of their DPIAs.

Responses were collected between March 6 and April 1, 2025, via *Nettskjema*, a web-based survey tool developed by the University of Oslo[1]. Potential respondents were contacted via email and social media platforms, including LinkedIn, to solicit their responses. The email invitations leveraged professional associations and the network of experts in the field. The survey was conducted per the ethical guidelines of the University of Oslo and assessed by the Norwegian Agency for Shared Services in Education and Research[2] for compliant use of personal data. In total, 30 responses were submitted, with one submission discarded because it provided contradictory answers.

The survey questions were primarily designed to learn about the structure and resources common in DPIA processes, while considering the deficiencies outlined in Sect. 3. The questions were primarily multiple-choice, with options for 'I don't know' and 'Other' to allow respondents to add more or less detail as needed. As the survey was anonymous, it first collected general information about the respondents' experience with DPIAs, the organisation in which they conducted the DPIA, and the regularity with which DPIAs occurred. These questions aimed to gauge the respondents' perspective and their familiarity with the DPIA as a process. The following questions then address the contents of the DPIA in the respondents' organisation. The goal was to determine if an unofficial standard could be identified by inquiring about the methods used in different

[1] https://nettskjema.no.
[2] https://sikt.no/.

phases of the DPIA. For this purpose, questions regarding the composition of the DPIA team, the tools used, threshold analysis, risk assessment, and identification of measures to mitigate the risk were included. The next section of questions focused on the compositional aspects, addressing the inclusion of third parties during different stages of the DPIA. The final questions requested details about the DPIA report and its overall result, including the quality and challenges faced during the entire process. For the challenges, only three answers were allowed to assert that a priority can be derived.

The complete questionnaire and results are available on github[3].

5 Results

In the following section, we present the aggregated results of the survey responses. To increase readability, the percentages will be rounded to the next integer. The total number of responses considered in the results is 29. The results are grouped into seven different categories: (1) general information about the respondent and their organisation, (2) general structure of the DPIA, (3) threshold analysis, (4) risk assessment and identification of measures, (5) third-party cooperation, (6) DPIA result, and (7) challenges in the DPIA process.

5.1 General Information

While the survey was anonymous, some basic information about the participant and their organisation was collected to provide some context to the answers.

Concerning information about the respondents, they were asked about the roles they typically fulfil during a DPIA and their experience with the process. The majority of respondents, 38%, are Data Protection Officers (DPOs). The next largest group are legal advisors with 14%, followed by project leaders, specialists in relation to the use case of the process to be assessed by the DPIA, IT experts, and external DPIA experts with 10% each. Further, a manager and chief privacy officer participated. The relevance of DPIAs, even before the GDPR came into force, is evident in the respondents' experiences. 38% work with DPIAs for seven to nine years already, with 7% having ten or more years of experience. 38% of participants started working with DPIAs shortly after the GDPR entered into force, having three to six years of experience. There were also some newcomers, with 14% having one to two years of experience and one respondent working with DPIAs for less than a year.

Regarding the organisations the respondents are part of, 45% of organisations work in commercial services, such as e-commerce, banking, or software development, while 34% work in public services and 21% in education and research. Roughly a third of these organisations are SMEs, with 21% having between 50 and 250 employees, 10% having ten to 50, and one organisation employing less than ten persons. Consequently, the rest are large organisations with 62% having 1000 or more employees and one organisation having between 251 and 999.

[3] https://github.com/Hinnaaak/DPIA_User_Survey.

Conducting a DPIA does not appear to be a one-time thing for most organisations, with only one having conducted a single DPIA in the last five years. 7% conducted two to four, 24% five to ten, 28% eleven to 25, and 34% more than that. One respondent did not know how many DPIAs their organisation had done in the last 5 years. If we take a look at only the last year instead, we get 14% with one DPIA, 34% with two to four, 31% with five to ten, 7% with eleven to 25, and 14% with more than that.

5.2 General Structure of DPIAs

The first step in understanding the structure of DPIA processes in organisations is to know who carries out the DPIA. To provide an example of the composition of a DPIA team, we can take a look at the UK's ICO. They recommend including the business area or project leader, DPO, information security staff, data processors, and legal advisors, as well as other relevant experts [33]. Furthermore, the views of the affected individuals or their representatives should also be consulted.

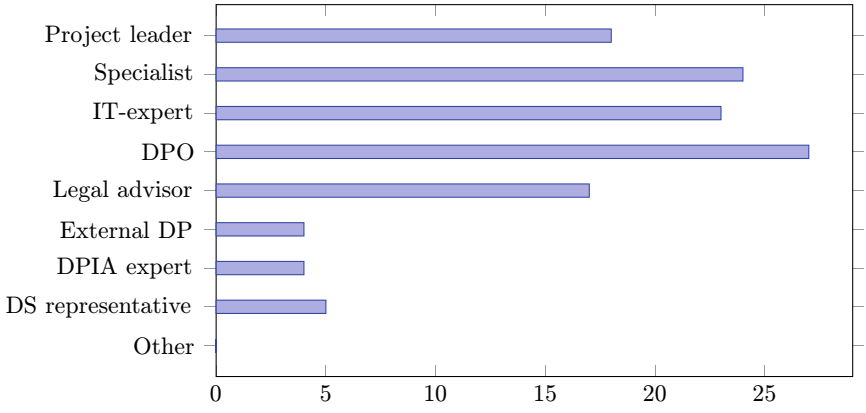

Fig. 2. Roles included in the DPIA process (n = 29)

The answers received do not necessarily follow these recommendations by the British supervisory authority, as 45% responded that their DPIA team consists of only two to four people. 34% reported a size of five to seven, roughly matching the ICO's recommendation. 14% invest more human resources, reporting teams of size eight to ten, while 7% go even bigger, working with ten or more people. Regarding the distinct types of people involved in the DPIA process, as illustrated in Fig. 2, we observe that the responses align with the recommendations in some areas, while deviating in others. Specialists for the use case, IT-experts, and DPOs are found in more than four-fifths of DPIA teams, and the project leaders and legal experts participate in roughly 60%. However, the roles often

located outside the organisation are not represented with the same frequency. Representatives of individuals and external processors are only included in 17% and 14% of the responses. External DPIA experts are also reported in only 14% of cases, indicating a low usage of external DPIA services.

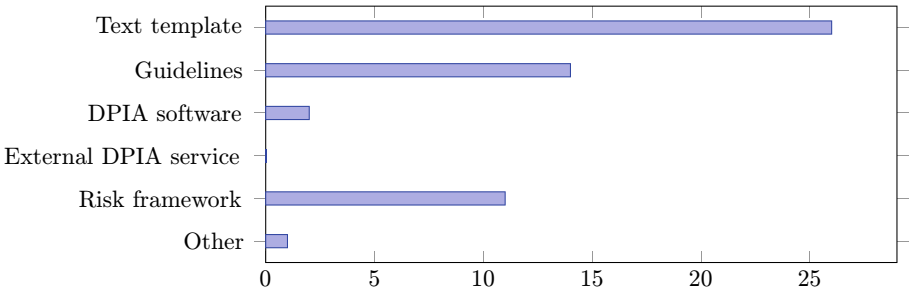

Fig. 3. Tools and aids used for a DPIA (n = 29)

Figure 3 illustrates the tools and aids utilised during the DPIA process, thereby confirming this assumption. No respondent stated that they use an external DPIA service in their organisation. Do keep in mind, however, that 10% reported themself as an external DPIA expert. Instead of external DPIA services, 90% rely on text templates for their DPIA. Additionally, organisations rely on official guidelines (48%) and risk management frameworks (38%) to conduct their DPIAs. While a variety of commercial DPIA software can be found online, only two respondents reported using DPIA software, and one stated they use AI. When asked for the specific tools they use, the majority responded with a self-developed solution (55%) or a self-developed template derived from a template or guideline (10%). 17% instead use a provided template directly. These templates originate from various sources, including governments and municipalities, supervisory authorities, and sector-specific shared resources, such as templates for hospitals.

5.3 Threshold Analysis

Nägele et al. critiqued that DPIAs are often conducted for processes that do not require a complete DPIA [5]. The question arises how the threshold analysis for DPIA looks in practice. According to the answers we received, 45% of respondents follow up with a complete DPIA on roughly a quarter of processes screened. 24% each report half and three-thirds of processes respectively, while 7% conduct a complete DPIA for every process.

The factors used to arrive at the conclusion are shown in Fig. 4. The 7% that follow up on every screening can be seen here as well. The most prominent factor, however, is the checklist with 86%. Following a checklist for processing activities that are likely to result in a high risk to individuals during the threshold

analysis can also be found in many guidelines, such as those released by the EDPB [9]. Guidelines in general impact the outcome of the screening for 76% of organisations. Going away from tools used in the threshold analysis, discussion within the DPIA teams is the most frequent factor with 55%, while the decision is left to the DPO in 45% of cases. Rarely (10%), external consultants are brought in to provide an additional perspective.

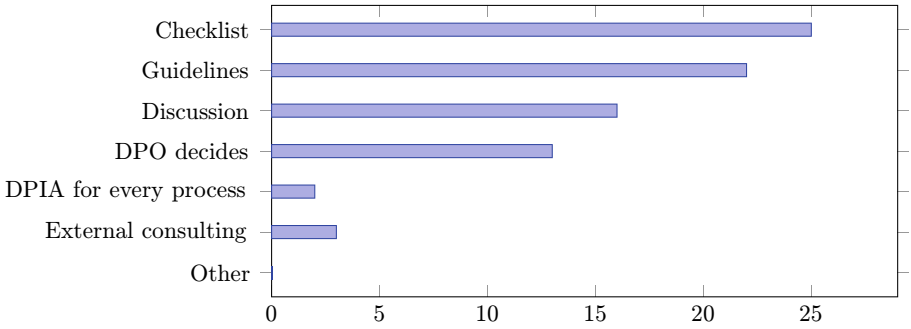

Fig. 4. Factors used to decide if a complete DPIA is mandatory (n = 29)

5.4 Risk Assessment and Measures

Risk assessments can be highly complex and are therefore hard to accurately gauge with a quantitative survey approach. Instead, we asked for the tools and aids used to identify both risks and measures. The most prominent methods to identify risks (see Fig. 5) are risk management frameworks, internal lists of risks, and internal consulting, which are utilised by roughly two-thirds of respondents each. Further, internally utilised methods include discussions (55%) and threat modelling (38%). Further, 31% use other DPIAs as reference. While it is not clear if these DPIAs are internal or external, based on the responses in Sect. 5.6, we can assume that these are more often internal. External risk guidelines are used in approximately one-third of cases, with the 'Other' response being similar to an external guideline. Online searches (21%) and external consulting (17%) are other sparsely used examples of getting information from outside.

If we compare the methods to identify measures for the risks (see Fig. 6) to these numbers, established technical and organisational measures and an internal list of measures are prominent as well, with 72% each. Discussions were stated the same number of times, increasing their relevance by 17% in comparison to the risk identification. Organisations from the public sector and research and education are especially fond of discussions, with three-thirds using them for risk and 94% for measure identification. Guidelines (48%) and other DPIAs (41%) increase in relevance as well, while online searches (14%) get used slightly less. Internal consulting, on the other hand, is used only 38% instead, while external consulting received the same number of responses as before.

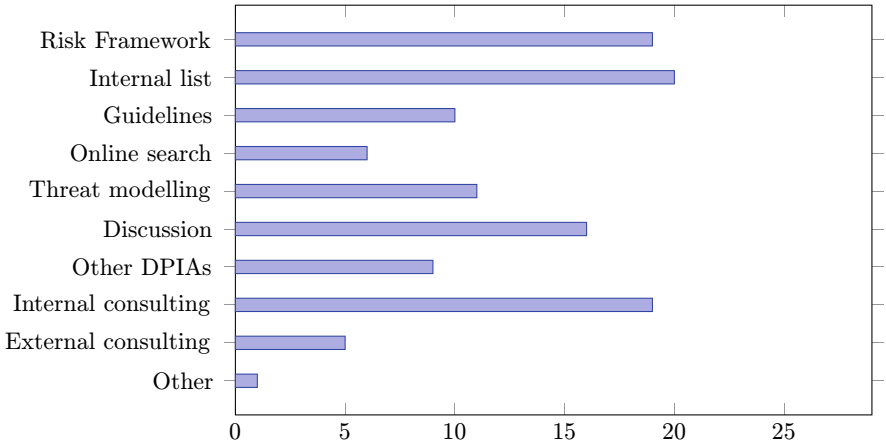

Fig. 5. Tools and aids used to identify risks (n = 29)

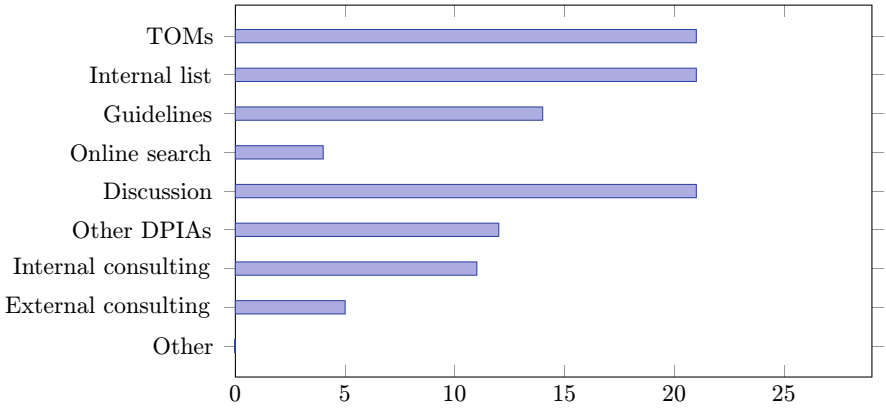

Fig. 6. Tools and aids used to identify measures (n = 29)

5.5 Third-Party Cooperation

The answers in Sect. 5.2 have shown that DPs are rarely included in the DPIA teams. That does not mean they are not considered during the DPIA. 86% stated that they request information from external DPs where they are involved in the processing activities, and 69% further request a list of risks and measures from them. To provide some additional information, Fig. 7 illustrates the parts of the DPIA where the third party is involved. The organisations do the screening exclusively by themselves, and only receive external input for the DPIA report in 10% of cases. Rougly a third of the time, third parties are involved during the process description (38%) and evaluation (31%). The aspects where organisations communicate with their collaborators the most are the risk assessment (48%) and identification of measures (45%). While 34% of respondents stated they do

not include third parties during any stage of the DPIA, 60% of them still request information from them where they are involved in the processing.

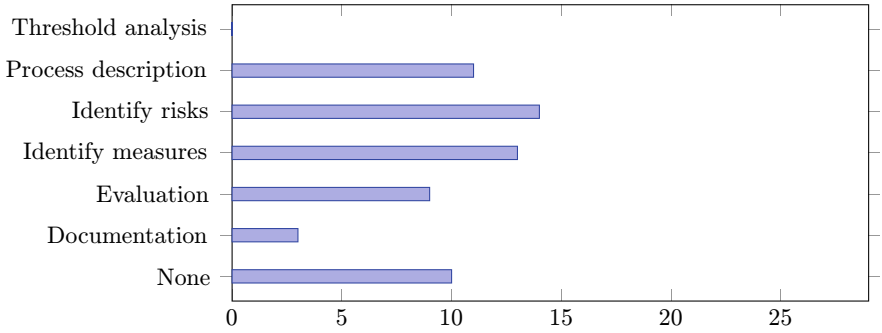

Fig. 7. Where representatives from third parties are involved (n = 29)

Besides DPs there is also the case of joint controllership, which can be tricky to address in a DPIA as it is not clear how the shared responsibility impacts the requirements for the DPIA process. From the 38% of respondents that were involved in a DPIA for processing activities with joint controllership, 40% stated they have agreements in place to distribute the responsibility between the parties, while 20% hold discussions between the two parties to address this issue. Another 20% decide depending on the circumstances, giving the main responsibility to the controller with more control over the processing or the one with more resources and expertise. One respondent's organisation resolves the shared responsibility by allowing each controller to conduct their own DPIA.

5.6 DPIA Results

While the GPDR demands a report to document the results of the DPIA, the format is not strictly defined. 69% of respondents document the DPIA result in text form only, while the rest additionally provide it in a structured data format.

As shown in Sect. 5.4, other DPIA results can be a valuable resource during the identification of risks and measures in a DPIA. The existence of a DPIA for a comparable processing activity might further relieve an organisation from the requirement to conduct a DPIA. Hence, sharing DPIA results can be advantageous. However, only 7% make their DPIA results publicly available and 41% share them with external stakeholders on request. Sharing results is more popular in larger organisations. 11% of respondents from organisations with 1000 or more employees reported about publishing their results, and 56% share results on request.

Another important aspect of the DPIA is its cyclical nature, requiring regular review and reevaluation of the DPIA results. Figure 8 shows when respondents review a DPIA. One common trigger for a review is the time passed. 55% report

they review a DPIA after a specified time frame of once per year or more often, while 17% have a time frame of less than once per year. Another trigger is changes to either the process (59%) or the information system (52%). A security breach leads to a review of DPIAs in 24% of cases, while 7% report that they do not review their DPIAs at all.

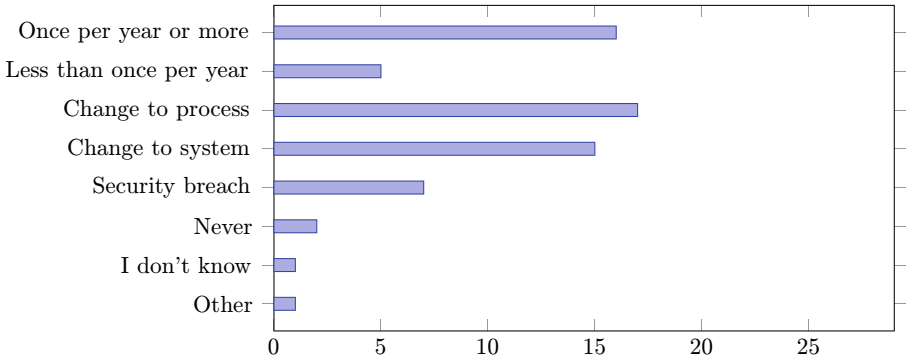

Fig. 8. When DPIAs are reviewed (n = 29)

Finally, the respondents were asked about their confidence in the DPIA result (see Fig. 9). Overall, participants appear to think that their DPIA process yields a somewhat satisfactory result, with no one reporting an inferior outcome and only one respondent categorising their DPIAs as poor. 38% report their results as acceptable, and the majority thinks their work is good (34%) or very good (24%).

5.7 Challenges

While the questions above primarily aimed to identify common patterns during the DPIA process, we were also interested in what the respondents identified as

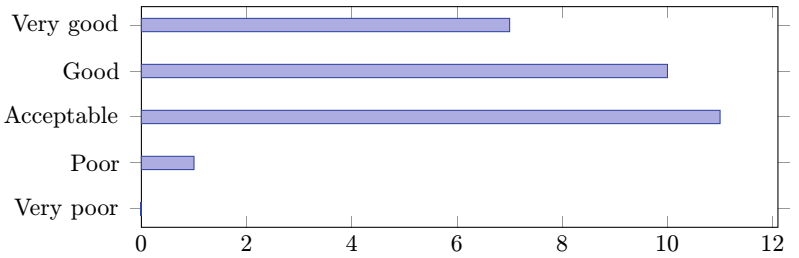

Fig. 9. Confidence in the result of the DPIA (n = 29)

the most significant challenges they faced during the DPIA process. Up to three challenges could be given. The responses are displayed in Fig. 10.

The two biggest challenges stated were the complexity of data processing activities (79%) and lack of time (59%). Overall, organisations struggle with different types of deficiencies, with a lack of budget (14%), expertise (24%), and adequate DPIA tools (24%) all receiving some attention. The identification of risks and measures was also highlighted as problem areas in 17% and 28% of responses, respectively. Unclear legal requirements are seen as a major issue by 14% of participants. Finally, one respondent complained about a lack of knowledge from third parties, and another one criticised the overall culture surrounding DPIAs, leading to a tedious and conservative DPIA process.

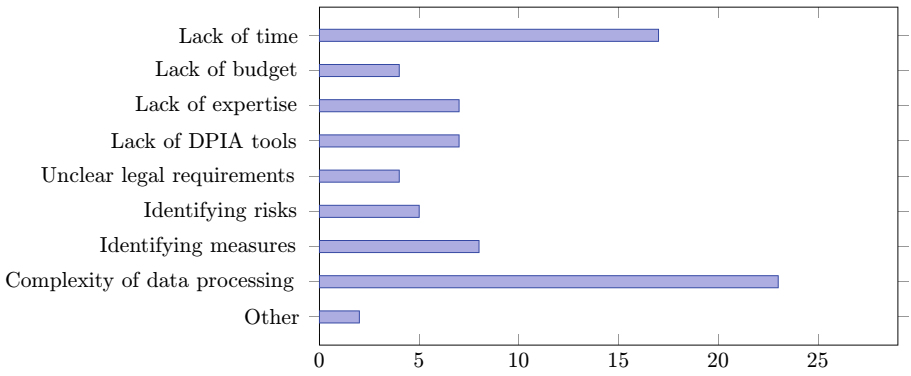

Fig. 10. Biggest challenges during a DPIA (n = 29)

6 Analysis and Discussion

6.1 Reusability of DPIAs

Given the substantial resources invested in the DPIA process, reusing the results or parts of them is desirable. When a process is sufficiently similar, a previous DPIA can even completely exempt the DC from the requirement for a DPIA.

Almost all respondents report that their organisation conducts multiple DPIAs per year. While using other DPIAs to identify both risks (31%) and measures (42%) is common, it is not a standard procedure. Apart from internal sources, the DPIA results of other organisations can also be used as a reference. This is especially important for types of processing that the organisation has no previous experience with. With only 7% of respondents sharing their DPIA results publicly and 41% sharing them on request only, which requires information about the existence of this DPIA, obtaining external references is challenging.

The specific combinations of types of processing and data used, an organisation's information system, and other relevant criteria influence the risks, measures, and general outcomes of a DPIA. Considering the size of the European data ecosystem, the correlations between these criteria are most likely not unique. Other DPIA results can therefore be a valuable tool for improving the quality of results and alleviating a lack of time and expertise. Further research should examine how DPIA results can be made publicly available, e.g., in the form of an open repository, without creating more risks or disclosing confidential information of the organisations.

6.2 Cooperation and Compositional Aspects

While external processors become involved at various stages of the DPIA process (see Fig. 7), Fig. 2 illustrates that they are rarely part of the DPIA team. As most organisations request information from involved processors, an organisation judging the external party's contributions to the DPIA as irrelevant or unimportant is unlikely. However, with a lack of time and budget being prevalent challenges, and the DC having full responsibility for the DPIA, getting people not contracted to your organisation permanently involved can be difficult.

With external parties only sparsely getting involved, if at all, during the actual DPIA process, the question arises as to what information is being requested from them, especially in terms of completeness and comprehensibility. An issue that has recently been raised by ENISA [2] is risks stemming from the composition of actors involved in a processing activity. Addressing these risks requires communication and insights into the information systems from all parties involved. Whether the level of collaboration that is expressed by the respondents' answers is sufficient to meet these criteria is doubtful.

The biggest challenge during DPIAs, according to the participants, is the complexity of processing activities. The most effective approach for a DPIA process to handle this complexity is likely an improvement of the process description. The hardest parts of a process to describe for a DPIA team are probably those that are not located within their own information system. However, only 38% of respondents involve third parties during the process description.

Overall, more information is needed about the exact forms and contents of communication between collaborating parties during a DPIA. The impact of other existing legal mechanisms between the parties, such as data processing agreements, also warrants attention. Additionally, the inconsistent involvement of third parties warrants an investigation into how DPIA processes can be designed to facilitate external participation more effectively.

6.3 Review of DPIAs

As shown in Fig. 8, there are various triggers for a DPIA review. With changes to the process at 59% being the most prominent reason, a consistent pattern for when a DPIA gets reviewed is hard to spot across organisations. The GDPR

demands a review of the DPIA *"at least when there is a change of the risk represented by processing operations"* [1, Art. 35(11)]. Complementary, the guidelines by the EDPB [9] recommend reviewing periodically, after a change to the legislation, or a change to the processing operations. Especially changes to the process might incur changes to the risks, as consequences are hard to estimate beforehand. This strict interpretation would make a revision of the DPIA mandatory after a change to the process, and thus 41% of respondents would be non-compliant. You can argue the same way for organisations that do not engage in periodic reviews. The question arises, why does the review process appear to be lacklustre? This issue requires further investigation into the approach taken by organisations. It can be assumed that stricter guidelines and a clearer definition of when a change to the risks occurs are needed. For which changes to the processes do changes to the risk apply as well, and how do other triggers, such as changes to the system or a security breach, correlate with it?

Data spaces, as an emerging data ecosystem, face additional challenges regarding a DPIA review due to changes in the process. The external parties involved in data sharing for a process can change dynamically within a data space. These dynamically changing third parties all have their own local risks and might introduce new compositional risks. These risks would need to be shared and assessed each time, highlighting the need for automating the review of these changes to the process.

6.4 Experience with DPIAs

The majority of respondents have multiple years of experience with DPIA processes. Their familiarity with the procedure might diminish the impact of some challenges and issues on the process. The respondents stated that the complexity of processing activities is the biggest challenge. This leads to the assumption that this issue might be systematic rather than stemming from a lack of expertise. The four respondents with 1 to 2 years of DPIA experience all stated a lack of time as a major challenge. Three of them also criticised the existing DPIA tools. Although the sample size is small, a learning curve can be assumed, as familiarity with the process and tools is expected to improve efficiency and consequently reduce the time required for a DPIA. However, the reason for stating a lack of tools as a challenge can also stem from an insufficient quality of the tools. Interestingly, the one respondent with less than a year of experience did not provide either a lack of time or tools as one of the three biggest challenges, further warranting additional research in the influence of experience on the DPIA process.

6.5 DPIA Culture

At the level of organisation conducting DPIA Processes, awareness of privacy and security issues related to the handling of large amounts of data is crucial for data protection practices [34]. The potential of DPIA, therefore, lies not only in its use as a technical or legal instrument but also in its ability to foster

a culture of data protection within organisations. The data protection culture addressed here encompasses internal awareness and sensitivity to data handling, as well as the development and implementation of principles, rules, and roles within the organisation [35,36]. The involvement of third parties, particularly in identifying risks, can be considered supportive, but there is also a risk of compromising internal sensitivity to organisation-centred risks (see Fig. 7). It is also important for an organisation to be aware of the specific types of data involved in the DPIA and what their materiality means for the handling of that data. At the individual level within organisations, skills in handling data appear to be crucial for the DPIA process.

A culture of data protection can be seen as a significant factor in the effectiveness of the DPIA, as it creates a framework within organisations in which the responsible handling of data is embedded as a value in data protection practice, thereby going beyond the fulfilment of legal requirements. This culture becomes visible when data protection is understood in practice as an integral part of corporate strategy, supported by organisational measures, and prioritised. As Fig. 5 shows, the organisational framework for a DPIA appears to be uncertain at present. In addition to procedural challenges such as the complexity of data processing, the factors of time, expertise, budget, and a systemic approach are considered particularly challenging organisational parameters.

6.6 Interaction Between the DPIA and Other Legislation

A relevant aspect outside the survey's scope is the interaction between the DPIA and legislation other than the GDPR. The impact of other current and potentially future legislation must be considered in the design of DPIA processes.

Kelemen and Hohmann [37] have demonstrated similarities between the DPIA and the obligations for risk assessment related to services and systems used by very large online platforms under the Digital Services Act [38]. Another novel piece of legislation is the AI Act [39], which introduces the Fundamental Rights Impact Assessment (FRIA) for high-risk artificial intelligence systems. The requirements for FRIA and DPIA overlap on multiple occasions, and the automation and reusability aspects of the DPIA could serve as an extension to the FRIA [40]. Initial approaches to a framework for identifying synergies between DPIAs and FRIAs have already been discussed [41]. Further, a tool that reuses DPIA results in FRIAs has been introduced [42]. While these approaches focus on how DPIAs can be used to supplement a FRIA, the question of how the FRIA and other legislation might impact the DPIA process remains.

As we advance, interactions with the risk assessment obligations under other legislation must be examined more closely. Matching requirements and procedures between the different risk assessment frameworks is potentially symbiotic. This can simplify the complexity stemming from the various legal requirements and complement both results.

6.7 Limitations

This research is subject to some limitations. First, the design of questions can introduce some bias. Most questions were either single or multiple-choice questions with pre-defined options. While we attempted to make these options as comprehensive as possible and included an *Other* option, it cannot be ruled out that respondents may have omitted some niche practices because they were not included in these options.

Since the survey was anonymous, the possibility of malicious answers or multiple submissions exists. We decided to accept this risk because there is no real incentive to manipulate the results.

Another issue is the sample size and difficulties in reaching possible respondents. The target audience is specific, and while many people may have been consulted for a DPIA in the past, they don't necessarily feel sufficiently involved with DPIAs to respond to the call for participation. Additionally, we did not find any DPIA-specific communities. This increased the reliance on networks and communities related to the broader field of privacy, data protection, and GDPR compliance. This might have introduced another bias in the results, as these participants are likely more involved with the topic than the average member of an organisation. Further, the small sample size made it challenging to identify correlations between the group of respondents.

Lastly, the survey's quantitative design means that the insights into the respondents' DPIA process are rather superficial. While we can draw meaningful conclusions about general trends and challenges regarding DPIA procedures in organisations, we did not obtain information about how a specific step of the DPIA is executed or what DPIA results look like. Further research is needed to address this gap and enable us to develop improvements for the DPIA process. Expert interviews, participating in a DPIA process, and collecting DPIA results from various sources may be reasonable next steps to address this issue.

7 Conclusions and Future Research Directions

As can be seen from our survey results, the implementation of data protection impact assessments remains somewhat heterogeneous in the European landscape, with a tendency to implement ad-hoc rather than formalised DPIA processes. Most survey respondents confirmed the utilisation of non-standardised DPIA methodologies, or the use of existing methods at the level of guidelines rather than a formal approach or tool. Individual, hand-written text documents make up the majority of DPIA reports, inspired by templates published by data protection authorities or domain-specific organisations.

Our survey also revealed that while third parties (external processors) are often requested to provide information about their data processing approaches and DPIA risk inputs, they are typically not actively involved in the DPIA process itself. The biggest challenge here lies in the complexity of data processing, which often renders a comprehensive DPIA process—covering all stakeholders and risk sources—unfeasible in terms of time and resources.

Based on our analysis of the survey results, it would be worthwhile to analyse different approaches to standardisation, formalisation, and (semi-)automation of the DPIA process to reduce efforts and improve quality, comparability and interoperability. We further plan to identify different DPIA cultures and the socio-technical factors that determine the DPIA process. Finally, we will develop a generic DPIA process repository that can serve as a template library for ongoing DPIA processes.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

Appendix

Questions and answer options of the survey:

1. How many years of experience do you have in DPIAs or privacy impact assessments in general? None; Less than a year; 1–2 years; 3–6 years; 7–9 years; 10 or more years

2. Which role do you primarily have during a DPIA? Project leader; Specialist (In relation to the use case of the process the DPIA is conducted for); IT-Expert (e.g. cybersecurity or sys-admin); Data Protection Officer; Legal advisor; External Data Processor representative; External DPIA expert; Representative of the affected individuals (e.g. works council); Other

3. Which sector does your organisation belong to? Commercial Services (e.g. e-commerce, banking, insurance, software development or consulting); Public Services (e.g. healthcare, public transport, law enforcement); Manufacturing; Agriculture, Food, Forestry, and Mining; Education and Research (commercial or public); Other

4. How many employees does your organisation have? 1–9; 10–50; 50–250; 251–999; 1000 or more

5. How many DPIAs did your organisation conduct in the last 5 years? 0; 1; 2–4; 5–10; 11–25; 25 or more; I don't know

6. How many DPIAs does your organisation on average conduct in a year? 0; 1; 2–4; 5–10; 11–25; More than 25; I don't know

7. How many people are on average involved in the DPIA Team in your organisation, including externals? 1; 2–4; 5–7; 8–10; More than 10; I don't know

8. Which roles are included in the DPIA process? Project leader; Specialist (In relation to the use case of the process the DPIA is conducted for); IT-Expert (e.g. cybersecurity or sys-admin); Data Protection Officer; Legal advisor; External Data Processor representative; External DPIA expert; Representative of the affected individuals (e.g. works council); Other

9. Which tools or aids do you typically use for a DPIA? Text template; (Official) guidelines; DPIA software; External DPIA service; Risk management framework; I don't know; Other

10. Please give the name of the tools or aids you use (free text response)

11. After conducting the threshold analysis, which fraction of processes require a complete DPIA? None; Roughly 50

12. How do you decide a complete DPIA is mandatory when evaluating processing activities? Checklist; (Official) guidelines; Discussion with the DPIA team; The DPO decides; We do a DPIA for every process; External consulting; I don't know; Other

13. Which methods do you use to identify possible risks? Risk Frameworks; Internal list of risks; External list of risks/guidelines; Online search; Threat modeling; Discussion; Other DPIAs; Internal consulting; External consulting; I don't know; Other

14. Which methods do you use to identify measures to address the risks? Established technical organisational measures; Internal list of measures; External list of measures/guidelines; Online search; Discussion; Other DPIAs; Internal consulting; External consulting; I don't know; Other

15. In which parts of the DPIA process do you typically involve representatives from third parties? Threshold analysis; Process description; Identify and assess risks; Identify measures to mitigate risks; Evaluation of the DPIA; Documentation of results; I don't know; None

16. Do you request information from external Data Processors where they are involved in the Processing Activities? Yes; No; I don't know

17. Do you request a list of risks and measures or a DPIA from external Data Processors where they are involved in the Processing Activities? Yes; No; I don't know

18. Did you ever conduct a DPIA for processing activities with joint controllership? Yes; No; I don't know

19. In which form do you document the result of your DPIA? Text only (e.g. PDF); Structured data format only (e.g. JSON or XML); Text and structured data format; I don't know; Other

20. Are DPIA results shared with external stakeholders? Yes, publicly available; Yes, shared upon request; No, internal use only; I don't know

21. When do you review a completed DPIA? After a fixed period of time (1x per year or more often); After a fixed period of time (Less than 1x per year); After a change to the process; After a change to the information system (IT architecture); After a security breach; Never; I don't know; Other

22. How confident are you in the accuracy of the DPIA result on average? Very Poor; Acceptable; Very Good

23. What are the biggest challenges you and your organisation face during a DPIA? Lack of time; Lack of budget; Lack of expertise; Lack of adequate tools for DPIAs; Unclear legal requirements; Difficulties identifying data protection risks concerning the individual; Difficulties identifying adequate data protection measures; Complexity of data processing activities; Other

References

1. European Parliament and Council: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Visited 25 Jan 2024
2. Drogkaris, P., Prieto, J.G. (eds.): European Union Agency for Cybersecurity: Engineering Personal Data Protection in EU Data Spaces (2024)
3. Curry, E., et al.: Data sharing spaces: the BDVA perspective. In: Otto, B., ten Hompel, M., Wrobel, S. (eds.) Designing Data Spaces: The Ecosystem Approach to Competitive Advantage, pp. 365–382. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-93975-5_22
4. Agencia Española de Protección de Datos: APPROACH TO DATA SPACES FROM GDPR PERSPECTIVE (2022). https://www.aepd.es/documento/approach-to-data-spaces-from-gdpr-perspective.pdf. Visited 27 June 2024
5. Nägele, P., Petrlic, R., Schemmel, F.: Die Datenschutz-Folgenabschätzung in der Praxis. Datenschutz und Datensicherheit - DuD **44**(11), 719–728 (2020). ISSN: 1614-0702, 1862-2607. https://doi.org/10.1007/s11623-020-1356-3. http://link.springer.com/10.1007/s11623-020-1356-3. Visited 29 Apr 2024
6. Datenschutzkonferenz. Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO (2018)
7. Commission Nationale Informatique & Libertés: PIA, methodology (2018)
8. Friedewald, M.: Datenschutz-Folgenabschätzung: Chancen, Grenzen, Umsetzung. In: TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis/J. Technol. Assess. Theory Pract. **26**(1-2), 66–71 (2017). https://www.ssoar.info/ssoar/handle/document/68742. Visited 24 Jan 2024
9. Article 29 Working Party: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017)
10. Martin, N., et al.: The data protection impact assessment according to article 35 GDPR. In: Fraunhofer Institute for Systems and Innovation Research ISI (2020)
11. Information Commissioner's Office: Sample DPIA template. v0.3, February 2019. https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf. Visited 14 Mar 2024
12. Agencia Española de Protección de Datos: Template for data protection impact assessment report (DPIA) for private sector (2022)
13. Commission Nationale Informatique & Libertés: PIA, templates (2018)
14. Commission Nationale Informatique & Libertés: PIA, knowledge bases (2018)
15. International Organization for Standardization: Information technology — Security techniques — Guidelines for privacy impact assessment. Standard. International Organization for Standardization, Geneva, CH (2023)
16. 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., Ikonomou, 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
17. Hansen, M., Jensen, M., Rost, M.: Protection goals for privacy engineering. In: IEEE Security and Privacy Workshops, pp. 159–166. IEEE (2015)

18. Gonscherowski, S., et al.: Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO auf der methodischen Grundlage eines stan- dardisierten Prozessablaufes mit Rückgriff auf das SDM am Beispiel eines “Pay as you drive”-Verfahrens (V 0.10) (2017)
19. Haag, I., et al.: Datenschutz-Folgenabschätzung gemäßszlig; Art. 35 DS-GVO (2019). https://opusihandbuch.kronsoft.de/documents/DSFA-B3S-Gesundheitsversorgung-Art.35-DSGVO.pdf. Visited 24 Jan 2024
20. Kloza, D., et al.: Data protection impact assessment in the European Union: developing a template for a report from the assessment process. LawArXiv, October 2020. https://doi.org/10.31228/osf.io/7qrfp. https://osf.io/7qrfp. Visited 13 Dec 2023
21. 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)
22. Friedewald, M., et al.: Data protection impact assessments in practice: experiences from case studies. In: Katsikas, S., et al. (eds.) Computer Security. ESORICS 2021 International Workshops. LNCS, vol. 13106, pp. 424–443. Springer, Cham (2022). ISBN: 978-3-030-95483-3 978-3-030-95484-0. https://doi.org/10.1007/978-3-030-95484-0_25. https://link.springer.com/10.1007/978-3-030-95484-0_25. Visited 29 May 2024
23. Wairimu, S., et al.: On the evaluation of privacy impact assessment and privacy risk assessment methodologies: a systematic literature review. IEEE Access (2024). https://ieeexplore.ieee.org/abstract/document/10418587/. Visited 28 May 2024
24. Georgiadis, G., Poels, G.: Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: a systematic literature review. Comput. Law Secur. Rev. **44**, 105640 (2022). https://www.sciencedirect.com/science/article/pii/S0267364921001138. Visited 29 May 2024
25. Vemou, K., Karyda, M.: Evaluating privacy impact assessment methods: guidelines and best practice. Inf. Comput. Secur. **28**(1), 35–53 (2019). https://www.emerald.com/insight/content/doi/10.1108/ICS-04-2019-0047/full/. Visited 29 May 2024
26. Todde, M., et al.: Methodology and workflow to perform the data protection impact assessment in healthcare information systems. Inf. Med. Unlocked **19**, 100361 (2020). https://www.sciencedirect.com/science/article/pii/S2352914820301477. Visited 29 May 2024
27. Stevanovic, U., et al.: Data Protection Impact Assessment - An Initial Guide for Communities (2018)
28. López, C.T., Domingo, I.A., Torrijos, J.V.: Approaching the data protection impact assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems. In: Proceedings of the 16th International Conference on Availability, Reliability and Security, pp. 1–9. ACM, Vienna, Austria, August 2021. isbn: 978-1-4503-9051-4. https://doi.org/10.1145/3465481.3469207. https://dl.acm.org/doi/10.1145/3465481.3469207. Visited 29 May 2024
29. Wuyts, K., et al.: Effective and efficient privacy threat modeling through domain refinements. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing, pp. 1175–1178 (2018). https://dl.acm.org/doi/abs/10.1145/3167132.3167414. Visited 29 May 2024
30. Calvi, A.: Gender, data protection & the smart city: exploring the role of DPIA in achieving equality goals. Eur. J. Spat. Dev. **19**(3) (2022)

31. De, S.J., Métayer, D.L.: A refinement approach for the reuse of privacy risk analysis results. In: Schweighofer, E., Leitold, H., Mitrakas, A., Rannenberg, K. (eds.) Privacy Technologies and Policy. LNCS, vol. 10518, pp. 52–83. Springer, Cham (2017). isbn: 978-3-319-67279-3 978-3-319-67280-9. https://doi.org/10.1007/978-3-319-67280-9_4. http://link.springer.com/10.1007/978-3-319-67280-9_4. Visited 29 May 2024
32. Pandit, H.J.: A semantic specification for data protection impact assessments (DPIA). In: Towards a Knowledge-Aware AI, pp. 36–50. IOS Press (2022)
33. Information Commissioner's Office: How do we do a DPIA? ICO, 17 November 2024. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/. Visited 28 May 2025
34. Dubey, R., et al.: Big data and predictive analytics and manufacturing performance: integrating institutional theory, resource-based view and big data culture. Br. J. Manag. **30**(2), 341–361 (2019)
35. Salleh, K.A., Janczewski, L.: Technological, organizational and environmental security and privacy issues of big data: a literature review. Procedia Comput. Sci. **100**, 19–28 (2016)
36. Phillips-Wren, G., et al.: Business analytics in the context of big data: a roadmap for research. Commun. Assoc. Inf. Syst. **37**(1), 23 (2015)
37. Kelemen, B.K., Hohmann, B.: Is there anything new under the sun? A glance at the digital services act and the digital markets act from the perspective of digitalisation in the EU. Croatian Yearbook Eur. Law Policy **19**, 225–248 (2023)
38. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). Legislative Body: EP, CONSIL, October 2022. http://data.europa.eu/eli/reg/2022/2065/oj/eng. Visited 17 Feb 2025
39. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). Legislative Body: CONSIL, EP, June 2024. http://data.europa.eu/eli/reg/2024/1689/oj/eng. Visited 17 Feb 2025
40. Kokoulina, O.: Challenges in digital compliance: risk assessment and fundamental rights under the GDPR and the EU AI Act (2024)
41. Thomaidou, A., Limniotis, K.: Navigating through human rights in AI: exploring the interplay between GDPR and fundamental rights impact assessment. J. Cybersecur. Priv. **5**(1), 7 (2025)
42. Pandit, H.J., Rintamäki, T.: Towards an automated AI Act FRIA tool that can reuse GDPR's DPIA (2024)