Thriving on Future Education, Industry, Business and Society
15–17 May 2019
Piran • Slovenia
make learn
TIIM
Management, Knowledge and Learning
International Conference 2019
Technology, Innovation and Industrial Management

DATA PROTECTION IMPACT ASSESSMENT GUIDELINES IN THE CONTEXT OF THE GENERAL DATA PROTECTION REGULATION

Bodo Grütter
University of Applied Sciences and Arts Northwestern Switzerland, FHNW, Switzerland
bodo.gruetter@students.fhnw.ch

Bettina Schneider
University of Applied Sciences and Arts Northwestern Switzerland, FHNW, Switzerland
bettina.schneider@fhnw.ch

Abstract:
The European General Data Protection Regulation (EU GDPR) requires companies to carry out a so-called Data Protection Impact Assessment (DPIA) if the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. But how can it be determined whether a risk should be considered 'high' and thus makes a DPIA necessary? Furthermore, if a DPIA is required, how exactly should this be performed? In response to these questions, various guidelines concerning DPIA have been published. The aim of this paper is to give those affected by the new Data Protection law an insight into three current DPIA guidelines and to support them in implementing a GDPR-compliant impact assessment. To this end, each of the selected guidelines will be described, and evaluated in terms of GDPR compliance and DPIA feasibility, i.e. on the one hand, whether the guideline complies with the relevant GDPR articles, and on the other hand what tools are provided to facilitate the operational execution of a DPIA. The study results in an overall evaluation matrix, which shows that all three guidelines have different strengths and propose differing methods for DPIA implementation.

Keywords: Data Protection Impact Assessment, Privacy Impact Assessment, General Data Protection Regulation, risk to rights and freedoms, data protection, EU law

1. INTRODUCTION

Digitalisation and the accompanying new technologies, in particular the worldwide spread of the Internet, have changed the way personal data (e.g., name, social security number, customer data and much more) is handled. Our world is at a point where most data about individuals is created and processed electronically (Tankard, 2016, p. 5). The European Union (EU) has noticed this trend and reacted to it with the General Data Protection Regulation (GDPR), a regulation for the protection of natural persons and their personal data (GDPR Article 1 (1)). This new data protection law, which became applicable on 25 May 2018, unfolds extraterritorial effect, and refers to any data processing related to individuals who are in an EU member state – irrespective whether the data processing itself takes place in the Union or not. Violations of these regulations may result in immense fines (GDPR Article 83 (4-6)).

A recent case from France deserves attention as an example: In January 2019, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), imposed a fine of 50 million euros on the American tech company Google for lacking transparency and giving insufficient information to the data subjects (Cellan-Jones, 2019). In order to avoid such penalties, GDPR suggests considering data protection in the early stages of any envisaged processing operation. Article 35 (1) of the law defines the implementation of a risk assessment tool, the so-called Data Protection Impact Assessment (DPIA)[1]. A DPIA is a method of describing the processing of personal data and assessing its risks to natural persons (WP29, 2017, p. 4). It must be carried out in situations where data processing is likely to result in high risks to the rights and freedoms of natural persons, in particular when using new technologies (GDPR Article 35 (1)). This raises the question of in which concrete cases the risks to natural persons should be considered 'high' and how a DPIA must be carried out exactly. Since GDPR addresses this question only superficially, various data protection authorities and other organisations have set themselves the task of defining the DPIA more precisely. They provide further detailed guidelines regarding this risk assessment approach. So far, there is no comprehensive view of these different guidelines.

The objective of this paper is to give those affected by the new data protection law a deeper insight into three state-of-the-art guidelines and to help them implement a DPIA. As the main method to achieve this, an iterative literature review process, recommended by Saunders, Lewis and Thornhill (2009, p. 60), was conducted. As a first step, the GDPR requirements for a DPIA were investigated. The official GDPR articles and recitals were considered the primary source. The results of this first iteration served to identify criteria for the evaluation of existing DPIA guidelines. In a second iteration, suitable DPIA guidelines could then be selected for comparison. To this end, a literature search was carried out using Google Scholar and Web of Science. Based on a third iteration, in which the details of the selected DPIA guidelines were examined, an evaluation matrix was created. The matrix resulting from the identified criteria showed the strengths of the respective guidelines and enabled an overall assessment. The search terms used throughout this entire process covering a period until October 2018 were 'Data Protection Impact Assessment', 'risk assessment' and 'guideline' combined with 'GDPR'.

The rest of this work is structured as follows: In the next section, the concept of DPIA with its minimum requirements is defined. The evaluation criteria for the comparison are then derived from this and the selection of the three guidelines to be considered in more detail is justified. Next, each guide is presented with an emphasis on the subsequent assessment. The main result is an evaluation matrix, which allows the comparison of the three guidelines and leads to a comprehensive discussion and some conclusions.

2. BACKGROUND ON DATA PROTECTION IMPACT ASSESSMENT

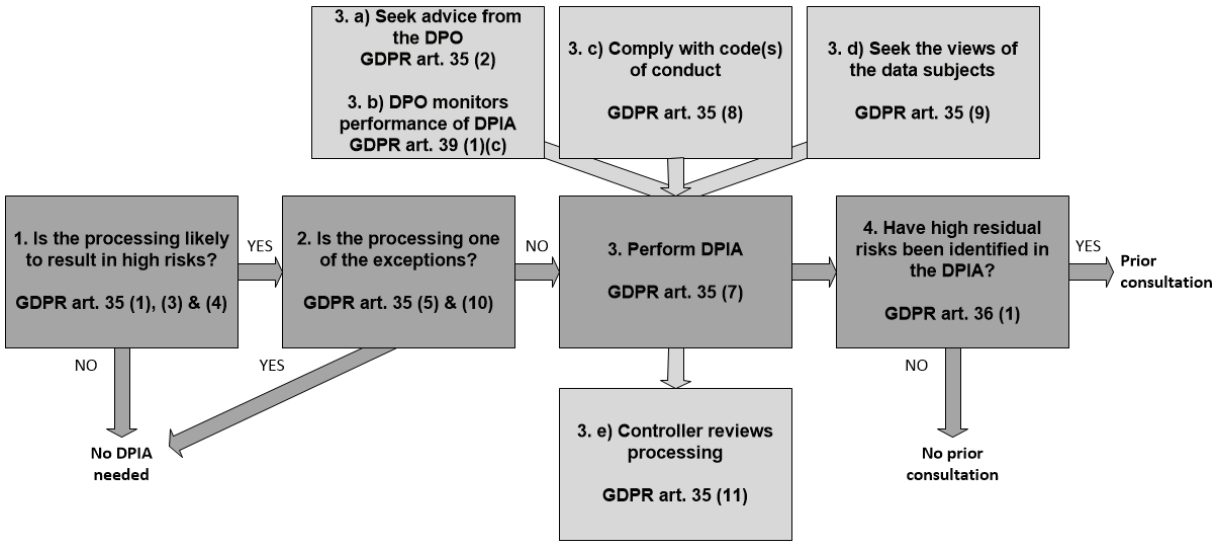
The processing of personal data may entail risks for individuals, also referred to as data subjects. Since GDPR pursues a risk-based approach, special attention needs to be paid to the concept of risk. Raphaël Gellert, who examines risks in relation to DPIA within the context of GDPR, presents two different perspectives: The first is describing the term risk in everyday language as a possible hazard that can only be predicted to a limited extent. The second is the technical use of risk to make decisions based on future events (Gellert, 2018, p. 280). In consequence, risks must be identified, described and

[1] Some references see the Privacy Impact Assessment (PIA) as synonymous, others treat it as a risk assessment tool with different assessment goals (Gellert, 2018, p. 286). The authors will stick exclusively to the term DPIA.

evaluated. A DPIA is a process designed to manage the risks associated with processing personal data by evaluating and determining measures to address those risks. Further tasks in the DPIA process are the description of the planned processing operations and an assessment of their necessity. In addition to complying with legal requirements, the DPIA has another central task. Companies that process personal data and use the DPIA to take mitigating measures prove that they take data protection seriously. This can create trust between society and potential customers (WP29, 2017, p. 4).

The DPIA is not an invention as part of the GDPR. A kind of DPIA was already mentioned in the predecessor of the new data protection law, the so-called EU guideline 95/46 (Gallotti, 2015). However, as a result of the GDPR, the DPIA will now become mandatory if the processing of personal data may lead to high risks for the rights and freedoms of natural persons (GDPR Article 35 (1)). Article 35 in the GDPR regulates the DPIA. Complements to it are found in Articles 36, 39 and in the recitals 74-77, 84 and 89-95. Among other things, it specifies when a DPIA is to be carried out, what it must contain at least, that certain codes of conduct must be observed, and which functions the roles of processor, controller and data protection officer (DPO) assume. Figure 1, elaborated in more detail in the following section, provides an overview of how the DPIA is structured in the GDPR and which basic principles it follows.

Figure 1: Structure of the GDPR related to the DPIA



Source: adapted based on WP29, 2017, p. 6

As the diagram shows, the first step in the DPIA process is to determine whether the risk of data processing results in high risks. According to GDPR, this applies to the following cases: Firstly, when a systematic and extensive evaluation of personal aspects is carried out on the basis of automated processing, which is used as input for decisions that significantly affect the individual; secondly, when personal data of special categories (e.g., data related to racial and ethical origin, genetic predisposition or sexual orientation) are processed on a large scale; thirdly, when systematic monitoring of publicly accessible areas is carried out on a large scale; and fourthly, if the processing appears in the list of DPIA-relevant processing operations and not in the exception list published by the competent supervisory authorities.

Correspondingly, high risks are examined in order to decide the exemption, i.e. whether the case is on the list of exceptions published by the competent supervisory authority or whether a DPIA has already been carried out for the specific processing operations and no DPIA is necessary at the discretion of the relevant EU Member States (step 2 in the diagram).

The third step in the process is the implementation of the DPIA. GDPR Article 35 (7) describes the minimum scope of a DPIA. It must contain at least a description of the planned processing operations, an assessment of their necessity and, proportionality, an assessment of the risks to the rights and freedoms of the data subjects and measures to address these risks. When carrying out a DPIA there are a number of things to consider.

On the one hand, various parties are involved: the processor, the controller, the supervisory authority and the DPO. The processor is a person or institution that carries out the processing of personal data. The data controller, who determines the purpose of processing and usually performs the DPIA, may conduct a review to assess whether the data processing is consistent with the established DPIA, where necessary. Where appropriate, the controller may also seek the views of the data subjects. The controller and processor may jointly designate a DPO that acts as a link to the supervisory authority and provides advisory services. If that is the case, the DPO will monitor the DPIA and advise the controller (GDPR Article 35 (2), (8), (9) & (11) and Article 39 (1)(c)). On the other hand, certain codes of conduct must be complied with in the performance of a DPIA in order to be able to apply the GDPR and demonstrate compliance (GDPR Article 35 (8)). Codes of conduct cover topics such as fair and transparent processing, the exercise of the rights of data subjects and the pseudonymisation of personal data (GDPR Article 40 (2)). If high residual risks have been identified in the DPIA, the controller asks for advice from the responsible supervisory authority, in a final step (GDPR Article 36 (1)).

3. EVALUATION CRITERIA AND DPIA GUIDELINE SELECTION

Based on the definition of the DPIA and the requirements of the GDPR, this chapter derives the evaluation criteria and selects three detailed DPIA guidelines for comparison.

3.1. DPIA Criteria for the Evaluation of the DPIA Guidelines

When deriving criteria for evaluating existing DPIA guidelines, it first seems important that the published guidelines comply with the GDPR requirements. The different DPIA approaches should – as a minimum condition – refer to the relevant DPIA Articles and describe the regulations as shown in Figure 1. Since the law offers a general binding framework rather than a detailed guideline with regard to DPIA, it also seems relevant to evaluate the existing state of detail of each DPIA guideline and to examine which instruments they offer to the companies concerned for implementing a DPIA in conformity with the law.

There are thus two main criteria, which are to be assessed: the compliance of the GDPR requirements and the DPIA feasibility by means of the guidelines (column headers of table 1). In order to assess the extent to which the DPIA guidelines apply to these two main criteria, additional sub-criteria are defined. These criteria are weighted (wt.) according to their importance on a scale from 1 (low priority) to 5 (high priority). Compliance with the GDPR requirements is regarded as the most important criterion with a value of 5. Tools provided by the guidelines to carry out the DPIA are considered as medium important criteria with a value of 3.

It is now necessary to define the concrete sub-criteria. The criterion GDPR conformity comprises compliance with all GDPR Articles (35, 36 and 39) as shown in Figure 1. The criterion DPIA feasibility covers different tools for the performance of the DPIA, which are not included in the GDPR: e.g., a more concrete description of when a DPIA must be performed. Table 1 gives an overview of the evaluation criteria.

Table 1: Evaluation criteria for comparison of the DPIA approaches

GDPR conformity			DPIA feasibility		
ID	Evaluation criteria	wt.	ID	Evaluation criteria	wt.
A1	Complies with GDPR Article 35 (1), (3) & (4)	5	B1	Provides concrete cases and examples where a DPIA is mandatory	3
A2	Complies with GDPR Article 35 (2)	5			
A3	Complies with GDPR Article 35 (5) & (10)	5	B2	Provides a described process for carrying out a DPIA	3
A4	Complies with GDPR Article 35 (7)	5			
A5	Complies with GDPR Article 35 (8)	5	B3	Provides tools for documenting a DPIA e.g., a template of a DPIA report	3
A6	Complies with GDPR Article 35 (9)	5			
A7	Complies with GDPR Article 35 (11)	5	B4	Provides checklists or similar tools that support the performance of the DPIA	3
A8	Complies with GDPR Article 36 (1)	5			
A9	Complies with GDPR Article 39 (1)(c)	5			

When applying the assessment grid to existing DPIA guidelines, the following results per criterion are possible: 1 for non-fulfilment, 2 for partial fulfilment and 3 for full fulfilment. The score per criterion is calculated by multiplying the resulting value by the weighting. The sum of all scores per main criterion results in the subtotal that is relevant for the assessment.

3.2. Selection of three DPIA Guidelines

As mentioned in the introduction, three DPIA guidelines published by different organisations were shortlisted in the literature review. One eligibility factor for selection was, on the one hand, that the guidelines answer the core questions of DPIA users, i.e. for which cases a DPIA is to be carried out and how the process may be implemented. On the other hand, it was also made sure that the content was not too similar, so that there would no longer be any added value when comparing the three directives. In other words, a selection criterion was that neither guideline is based on the other, but proposes its own approaches. A further qualifying factor was the origin of the guidelines. Therefore, one Europe-wide guideline, one national guideline and one guideline designed by two international standards organisations were selected (the latter in a variant enriched with concepts from another author).

The first selected DPIA guideline was published by the Article 29 Working Party (WP29). The WP29 is a former European advisory body – today known as European Data Protection Board (EDPB) – which has published various GDPR guidelines for the European Commission (European Data Protection Supervisor, n.d.). Their guideline is therefore very close to the new data protection regulation. The second DPIA guideline comes from the United Kingdom (UK) data protection authority, the Information Commissioner's Office (ICO) (ICO, n.d.). The third ISO/IEC 29134 guideline was published by the International Organisation of Standardisation (ISO) in collaboration with the International Electronical Commission (IEC). Their standard does not directly consider the GDPR. Mathias Reinis deals with ISO/IEC 29134 in his publication 'Privacy Impact Assessment according to ISO/IEC 29134 and its application within the GDPR'[2] in the context of the new data protection law GDPR and supplements it with further concepts (Reinis, 2017). Since this study aims to treat the DPIA in context of the GDPR, Reinis' publication of will be evaluated. This choice covers three DPIA guidelines, which originate from different organisations.

4. DPIA GUIDELINE DESCRIPTION AND ASSESSMENT

4.1. Description and Assessment of WP29's Guideline

The WP29 guideline is 22 pages long and comprises four chapters. The third chapter covers the main part of the guideline (WP29, 2017, p. 3). The first subchapter of the main part clarifies whether a DPIA addresses one or more processing operations. WP29 quotes GDPR Article 35 (1) and recital 92, which suggest that it may be more reasonable and economical to carry out a DPIA for more than one processing project. For multiple similar processing operations in terms of nature, scope, context, purpose and risks, only one DPIA is also considered sufficient. The DPIA may also be used to assess the data protection impact of technology products such as hardware or software. WP29 therefore references to GDPR Article 35 (1)(2), which states: "A single assessment may address a set of similar processing operations that present similar high risks" (WP29, 2017, pp. 7–8).

In the second subchapter, WP29 lists nine different situations where a DPIA becomes mandatory. Accordingly, a DPIA must always be executed if an evaluation and scoring, including predictions, is carried out based on the personal data. As soon as particularly sensitive data, such as health data or financial data, are processed, an automatic decision is made with serious implications for the data subjects or if they are systematically monitored, a DPIA is also necessary. Other cases, which require the implementation of a DPIA include the processing of personal data on a large scale, the processing of data relating to vulnerable persons and the innovative use of technological or organisational solutions. WP29 describes these nine cases in detail and supplements them with concrete examples. These listings are supplemented with a table, which contains concrete examples and decision criteria for assessing the necessity of carrying out a DPIA. Thus, WP29 answers the question of when processing can entail a high risk for the rights and freedoms of data subjects from GDPR Article 35 (1).

In addition, GDPR Articles 35 (3) and (4) are also clarified, in which WP29 sets out criteria for the data protection authorities that they can use to adapt their list, which precisely defines for the respective country when a DPIA is to be carried out (WP29, 2017, pp. 8–12). WP29 also deals with GDPR Article 35 (5) and (10). It mentions cases in which no DPIA is necessary. These include: If the processing is not likely to result in high risks for the rights and freedoms of the data subjects; if a DPIA has already been carried out for similar processing operations or before the GDPR came into force in May 2018; and if the processing operations are included on the optional list published by the responsible

[2] German original title: "Privacy Impact Assessment – Datenschutzfolgeabschätzung nach ISO/IEC 29134 und ihre Anwendung im Rahmen der EU-DSGVO".

supervisory authority (WP29, 2017, pp. 12–13). The lists when the DPIA is necessary and when not provide concrete cases and examples and therefore meet evaluation criterion B1: “Provides concrete cases and examples where a DPIA is mandatory”. In the third subchapter, it is clarified whether a DPIA must be carried out for already existing processing operations. WP29 states that a DPIA must be performed if the processing in EU Directive 95/46 has never been audited or has changed over time, e.g., due to new technologies and risks (WP29, 2017, p. 13).

The fourth subchapter describes the concrete implementation of the DPIA based on an iterative process. This process comprises seven activities: 1. description of the planned processing; 2. assessment of the necessity and proportionality of the processing; 3. taking measures already planned; 4. assessment of the possible risks; 5. taking measures to address these risks; 6. documentation of the DPIA; and 7. monitoring and review. This process is supplemented by the responsible roles, their tasks and the codes of conduct to be observed (WP29, 2017, pp. 14–19). Thus, WP29 also complies with evaluation criteria A2, A5, A6, A7, A8 and A9, i.e. GDPR paragraphs 35 (2), 35 (8), 35 (9), 35 (11), 36 (1) and 39 (1)(c). Hence, WP29 provides a described process for how a DPIA can be carried out under the GDPR and fulfils with this also evaluation criterion B2.

WP29 recommends publishing parts of the DPIA to build a trust with the data subjects. In the appendix, WP29 provides a checklist of various criteria which the data controllers (and their DPOs) can use to assess whether a DPIA is necessary or not, or whether a methodology for implementing a DPIA is sufficiently comprehensive to comply with the GDPR (WP29, 2017, p. 22). With this checklist, B4 is only partially fulfilled as it does not directly support performance, but rather serves as a tool for assessing processing operations and selecting methodologies. WP29 does not meet B3 because no template or standard outline for DPIA documentation is provided.

4.2. Description and Assessment of ICO’s Guideline

ICO offers a comprehensive guide to GDPR topics, which comprises 282 pages and deals with the DPIA in a separate chapter counting six pages and beginning on page 185. Only this DPIA chapter is considered in the description and assessment. On the first page, there is an ‘At a glance’ section. ICO mentions the most important points concerning DPIA. It describes, among other things, what a DPIA is, when it is to be executed and what minimum content it must contain (criterion A4). GDPR Article 35 (2) and (9) as well as Article 36 (1) (evaluation criteria A2, A6 and A8) require the controller to seek advice from the DPO, the data subjects and the supervisory authority. GDPR Article 39 (1)(c) (criterion A9) regulates the tasks of the DPO and states that the DPO has to offer advice on request within the framework of the implementation DPIA. ICO states that the DPO, if one has been designated, as well as the data subjects and other stakeholders such as experts must be consulted (ICO, 2018, p. 185). This also implies the advisory function of the DPO as required in A9. Therefore, this fulfils criteria A2, A6 and A9. A8 will be considered a number of pages later, in which ICO advises to consult them as the supervisory authority as soon as the DPIA identifies high risks and no measures can be taken to reduce them (ICO, 2018, p. 190).

ICO provides three different checklists on the first three pages of the DPIA chapter (ICO, 2018, pp. 185–187). In terms of evaluation, only the last two checklists should be described, as they deal with the questions of necessity and implementation of the DPIA. The second checklist lists the cases in which a DPIA must be carried out and when it should at least be considered. ICO lists the same cases as WP29 but adds another case. For example, ICO explicitly requires the implementation of a DPIA if no privacy notice, i.e. a statement on how personal data is processed, used and distributed, is provided to the data subjects. ICO does not list examples like WP29 but divides the cases into ‘must’ and ‘should’. Since the evaluation criterion is B1: "provides concrete cases and examples where a DPIA is mandatory", this criterion is evaluated with an average value. GDPR Article 35 (1), (3), (4), (5) and (10) (evaluation criteria A1 and A3) are fulfilled by providing this checklist. In general, ICO always recommends a DPIA. If one has decided against a DPIA, then one should document the reasons for it (ICO, 2018, p. 186). In the third checklist, ICO describes the implementation of the DPIA.

In addition, ICO represents a graphical DPIA process with the activities: 1. Identify the need for a DPIA; 2. Describe the processing; 3. Consider the consultation; 4. Assess the necessity and proportionality of processing; 5. Identify and assess risks; 6. Identify measures to mitigate risks; 7. Sign off and record outcomes; 8. Integrate outcomes into plan; and 9. Keep DPIA and processing under review. Thus, ICO also meets the evaluation criterion A8 and B2. In the chapter 'Data protection impact assessments' it is not explicitly mentioned that the codes of conduct of GDPR Article 40 are to be duly considered (GDPR Article 35 (8)) as in criterion A5. If one looks at the entire ICO guideline on GDPR, however, this is dealt with in a separate chapter 'Codes of conduct'. Therefore, there is a deduction in the evaluation. In addition to the checklists (criterion B4) as mentioned above, ICO also offers a downloadable template for a DPIA report (criterion B3).

4.3. Description and Assessment of Reinis' Guideline (based on ISO/IEC 29134)

Mathias Reinis first presents the environment of ISO/IEC Standard 29134 in his DPIA[3] guideline. He first presents the general structure of the ISO/IEC series of standards. Subsequently, the legal environment of the standard is already considered, i.e. GDPR Articles 35, 36 and 39. These articles are cited directly from the text of the law (Reinis, 2017, pp. 14–18). In addition, references to the new EU data protection law are made at certain points in the later chapters, e.g., in the DPIA process description (Reinis, 2017, p. 38). Thus, all evaluation criteria regarding GDPR conformity are considered as fulfilled.

In the second chapter, Reinis notes that ISO/IEC 29134 does not mention cases where a DPIA is required. ISO/IEC 29134, however, mentions four so-called 'fields of application' of a DPIA: 1. The definition of accountabilities where responsibility is shared between two or more organisations; 2. The implementation of a data protection risk management; 3. Assessment of the data protection risks arising from a project for which the later executor is not yet known. Research projects and legislative proposals are cited as examples; and 4. Demonstrate responsible behaviour towards the persons concerned, in particular in terms of social responsibility (Reinis, 2017, p. 24). This fact would not be sufficient yet for the evaluation, as the B1 evaluation criterion requires cases that are more concrete. Mathias Reinis however supplements the four fields of application with the examples which WP29 lists in its guideline (2017, pp. 19–20). This leads to B1 being fulfilled.

In chapter 4, Reinis discusses the implementation of the DPIA. He cites various roles and groups within the framework of the DPIA, which ISO/IEC list in their standard: The accepting person approves the DPIA report; Stakeholders are all internal or external parties involved in a DPIA; The assessor represents the person who directs and conducts a DPIA; The DPIA team supports the assessor in questions of DPIA content; Information recipients are a group of people who are allowed to read the DPIA report; The legal expert has experience in the fields of data protection law and supports the assessor (Reinis, 2017, pp. 34–37).

As in the other DPIA guidelines, an iterative process is described for this purpose. This process description comprises eight phases and defines for each phase the objective, the information requirements, the process steps in the phase and the process result. The eight phases are: 1. Check necessity of a DPIA; 2. Create a DPIA; 3. Information retrieval; 4. Involvement of stakeholders; 5. Identification and assessment of risks; 6. Determination of risk treatment; 7. Documentation and implementation; and 8. Review and adaption to changes (Reinis, 2017, pp. 36–67). This process description complies with evaluation criterion B2.

Reinis then devotes the last chapter entirely to reporting. He shows the reporting structure proposed by ISO/IEC 29134: Cover page; introduction; objectives of investigation; data protection requirements; risk estimation; risk treatment plan; conclusions and decisions (Reinis, 2017, p. 77). Thus, also B3 is fulfilled. Since Reinis does not provide any checklists or similar aids in his guide, B4 is judged with the lowest score.

[3] Reinis uses the term PIA as a synonym for DPIA.

5. RESULTS

The assessments elaborated in the previous chapter result in the following evaluation matrix.

Figure 2: Evaluation of the selected DPIA guidelines

	ID	Evaluation criteria	wt.	WP29		ICO		Reinis (based on ISO/IEC 29134)		
				Rating	Result	Rating	Result	Rating	Result	
GDPR conformity	A1	Complies with GDPR article 35 (1), (3) & (4)	5	3	15	3	15	3	15	
	A2	Complies with GDPR article 35 (2)	5	3	15	3	15	3	15	
	A3	Complies with GDPR article 35 (5) & (10)	5	3	15	3	15	3	15	
	A4	Complies with GDPR article 35 (7)	5	3	15	3	15	3	15	
	A5	Complies with GDPR article 35 (8)	5	3	15	2	10	3	15	
	A6	Complies with GDPR article 35 (9)	5	3	15	3	15	3	15	
	A7	Complies with GDPR article 35 (11)	5	3	15	3	15	3	15	
	A8	Complies with GDPR article 36 (1)	5	3	15	3	15	3	15	
	A9	Complies with GDPR article 39 (1)(c)	5	3	15	3	15	3	15	
				Subtotal	135	Subtotal	130	Subtotal	135	/135
DPIA feasibility	B1	Provides concrete cases and examples where a DPIA is mandatory	3	3	9	2	6	3	9	
	B2	Provides a described process on how to carry out a DPIA	3	3	9	3	9	3	9	
	B3	Provides tools for documenting a DPIA e.g. a template of a DPIA report	3	1	3	3	9	3	9	
	B4	Provides checklists or similar tools that support the performance of the DPIA	3	2	6	3	9	1	3	
		Weight: 1 = low importance ---- 3 = neutral importance ---- 5 = high importance		Subtotal	27	Subtotal	33	Subtotal	30	/36
		Rating: 1 = disagree ---------- 2 = partly agrees ---------- 3 = agree		Total	162	Total	163	Total	165	/171

Regarding the first main criterion, GDPR conformity, it can be recognized that all three guidelines have reached a high score. The evaluation guideline ICO suffers from the fact that only the considering chapter was judged. If one looks at the entire GDPR guideline, then also ICO would have received the full score. The second main criterion, DPIA feasibility, reveals larger differences. Of all three directives, WP29 focuses most on the question of when processing results in a high risk to the rights and freedoms of natural persons. The guideline offers a list with nine cases when a DPIA is required, a list with four cases when no DPIA is required and supplements this with specific examples. ICO provides three checklists with a different focus. The first deals with DPIA awareness, the second with the question when a DPIA should be conducted and the last with how this risk assessment should be carried out. Reinis considers the DPIA within the framework of the standard ISO/IEC 29134 and places it in the context of the GDPR. It is noticeable that in this guideline the focus lies on the implementation and documentation of the DPIA. Thus, about one third of the total number of pages is dedicated to this topic.

6. CONCLUSIONS AND OUTLOOK

This paper was written to help various companies or other organisations plan their data processing operations in such a way that the risks and consequences for data subjects can be assessed and, at best, treated. For this purpose, the DPIA was analysed in the context of the GDPR. By comparing different DPIA guidelines published by various institutions, their content and strengths (as shown in Table 2) should be highlighted. The third guide based on Reinis scored highest in the evaluation, but it soon turned out that there is no single winner.

All guidelines offer very different tools to perform a DPIA. The probably best solution is the combined use of individual guidelines, which complement each other. The recommendations published by the three different authors are intended to provide a framework within which the company can operate its own DPIA management. They should be adapted to the own company, not vice versa.

Table 2: Overview of the strengths of the selected DPIA guidelines

WP29	ICO	Reinis (based on ISO/IEC 29134)
Description and answer of ambiguities in the GDPR law. Provides a list of when the DPIA is necessary and when it is not. Explains the cases with examples.	Provides three checklists on the topics: DPIA awareness, screening and process. The guide covers the entire GDPR. DPIA is covered in one chapter.	Refers in all topics to the relevant ISO/IEC 29134 and GDPR sections. Describes every DPIA phase with: Objectives, information requirements, process steps and process results. Describes the DPIA documentation in a separate chapter. Provides a standard structure for a DPIA report according to ISO/IEC 29134.

It is recommended in all guidelines to publish the own DPIA reports in order to gain the confidence of the data subjects. The new data protection law is still relatively young. It can therefore be assumed that DPIA reports will be increasingly published over time. Looking to the future, these can be examined in further studies to identify best practices within the context of DPIA.

REFERENCE LIST

1. Cellan-Jones, C. F., Dave Lee, Rory. (2019, January 21). Google hit with £44m GDPR fine. Retrieved from https://www.bbc.com/news/technology-46944696
2. European Data Protection Supervisor. (n.d.). History of WP29. Retrieved from https://edps.europa.eu/data-protection/data-protection/glossary/a_en
3. Gallotti, C. (2015, July 21). The PIA concept from directive 95/46 to the current draft of the EU – Part 1 – Europrivacy. Retrieved 26 January 2019, from https://europrivacy.info/2015/07/21/pia-concept-directive-9546-current-draft-eu-part-1/
4. Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, *34*(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003
5. ICO. (n.d.). About ICO. Retrieved from https://icoumbraco.azurewebsites.net/about-the-ico/who-we-are/
6. ICO. (2018, August 2). Guide to the General Data Protection Regulation (GDPR). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/?template=pdf&patch=246#link34
7. Reinis, M. (2017). *Privacy impact assessment: Datenschutz-Folgenabschätzung nach ISO/IEC 29134 und ihre Anwendung im Rahmen der EU-DSGVO mit Schlagwortverzeichnis* (2nd ed.). Norderstedt: Books on Demand. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1867328
8. Saunders, M. N. K., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed). New York: Prentice Hall.
9. Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3
10. WP29. (2017, April 4). 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. Retrieved from http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236