Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality

Tamas Bisztray(✉) and Nils Gruschka

Department of Informatics, University of Oslo, Oslo, Norway
{tamasbi,nilsgrus}@ifi.uio.no

Abstract. Privacy and data protection have become more and more important in the recent years since an increasing number of enterprises and startups are harvesting personal data as a part of their business model. One central requirement of the GDPR is the implementation of a data protection impact assessment for privacy critical systems. However, the law does not dictate a special assessment methods.

In this paper we compare different data protection impact assessment methods. We have developed a comparison and evaluation methodology and applied this to three of the most widespread assessment frameworks. The result of this comparison shows the weaknesses and strength, but also clearly indicates that none of the tested methods fulfills all desired properties. Thus, the development of a new or improved data protection impact assessment framework is an important open issue for future work.

Keywords: Data protection · Privacy Impact Assessment · GDPR · DPIA

1 Introduction

Data is the new currency of the 21th century and there is an increasing number of businesses collecting and storing our personal information and making monetary benefits from it. The key to success for these businesses is to harness value from the collected data. To do this they need not just to store but to process what has been collected. Monetary benefits and business goals are easily pushing the protection of people's personal privacy down in the to-do list. The General Data Protection Regulation (GDPR) [8] was meant to give back the control to people over their private data.

Companies failing to fulfill requirements imposed by the GDPR can face serious fines laid out by Article 83 which in the worst case can be up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

If a company wants to avoid such high fines they have to adjust their operations to become compliant with the GDPR. However, many worry that these

A. Askarov et al. (Eds.): NordSec 2019, LNCS 11875, pp. 3–19, 2019.
https://doi.org/10.1007/978-3-030-35055-0_1

regulations are imposing an unnecessary burden on tech companies. This opinion was also voiced by Alibaba's founder Jack Ma who said in an interview: "Europe will stifle innovation with too much tech regulation" [18]. Indeed for a startup such a fine would be devastating. Allocating too much resources to become fully compliant could be similarly harmful. Therefore, becoming GDPR compliant from the beginning without too much hassle is very important. But more than a year after the GDPR came into force there still exists no standard framework in the EU and companies are either doing an assessment on their own or they have to find out which DPIA method is the one that would suit their project the best.

Article 6(1) contains six requirements one of which is necessary to fulfill in order to lawfully process PII (personally identifying information). One possibility is to obtain consent from the data subject. Article 7 further states that consent shall be requested in a way that is: *"clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language"*.

But what is intelligible, easy to understand plain language or what is appropriate in length can be matter of debate. Consent once acquired is very easy to demonstrate and allows the controller[1] to specify all use cases to rule out the possibility of unwanted legal issues. Whereas other requirements could be more difficult to prove.

Acquiring compliance therefore can look like one just have to ask something in a sophisticated way and if the user clicks accept the processing is lawful. Google's case serves as a counterexample where the company received a €50 million fine, inflicted by French data protection authorities (CNIL) [9]. According to CNIL the way Google obtained consent violated the transparency of obligations and was lacking legal bases. This case sets a good example but unfortunately, in practice there are still many instances where the users are presented sophisticated documents where copyright claims and other legal matters are mixed with asking consent without a clear description of the processing purposes.

There are several rules the data controller has to follow. Following our example with consent Article 7(3) says "*The data subject shall have the right to withdraw his or her consent at any time*". If the data subject withdraws consent for storing his personal information the data controller shall delete it. Meanwhile if the data was copied, shared with several processors, has been processed after which new PII was created, all of this has to be deleted, too. This requires that the data controller should constantly keep track of the data.

Obtaining and maintaining compliance with the GDPR requires attention and a good overview of operations related to PII. Improper management of PII can lead to the violation of the GDPR. This is specially challenging for companies with complex systems designed prior to the GDPR. Tackling this problem requires a method guiding organisations to identify and document activities related to personal data and assess risks related to its processing, while

[1] Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

providing steps to achieve compliance with the GDPR and the ability to demonstrate it. For this purpose Article 35 introduces DPIA (data protection impact assessment). Its a method that provides guided steps to identify and analyse how the rights and freedoms of individuals might be affected by certain actions or activities related to data processing, and to assist in avoiding/correcting these issues.

This paper will analyse and compare different DPIA methods. The goal of this work is twofold. Firstly, we are aiming to identify shortcomings of current DPIA methods. We will do this by proposing a metric that helps to identify advantages and disadvantages of existing methods. The second goal is to provide help for those who are planning to conduct a DPIA, but can't decide which framework would be the best for their application as of today. To help with this question we are briefly going through some frameworks highlighting their strengths and weaknesses.

Section 2 gives a general introduction to DPIA and an overview of the examined DPIA frameworks. Section 3 provides an overview of related work in comparing DPIA methods. In Sect. 4 we present our metric for comparing DPIA methods and perform the comparison itself. Section 5 contains the summary and conclusions.

2 Data Protection Impact Assessment

2.1 Legal Background

Data protection impact assessment is a new requirement under the GDPR as part of the *data protection by design and by default* principle (introduced in Article 25). According to Article 35:

> *If the processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations.*

Unfortunately it does not specify which type of processing requires a DPIA. The reader might be confused right from the start after finding these methodologies under the name of Privacy Impact Assessment (PIA). In practice they are the same concept. Originally PIA was only aiming to assess the privacy risks of a processing, whereas the GDPR requires DPIA to go beyond and determine sufficient security measures and safeguards to address these risks. As pointed out by Roger Clarke [12] in his *Comprehensive Interpretation of Privacy*, data privacy is just one of the four aspects of privacy where the other three are: privacy of the person, privacy of personal behaviour and privacy of personal communications. In this paper we prefer the use of DPIA over PIA but they are treated as synonyms.

In the *Guidelines on Data Protection Impact Assessment* published by the Article 29 working party nine criteria for processing likely to result in a high risk scenario (and therefore requiring a DPIA) are defined [1]. Similarly there is

a list of cases in which no DPIA is required. The general guideline is that if you are not sure where a certain process belongs a DPIA has to be performed.

Furthermore, Article 35(11) requires that a new DPIA has to be carried out when there is a change related to the risk of the process. This means that processes must be tracked over time in order to detect these kind of changes. This also applies to processes which are at the moment labeled low risk since the risk might change to high.

The GDPR does not reference a concrete DPIA method, but Article 35(7) at least defines the minimal content of a DPIA:

- *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
- *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;*
- *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

Therefore, no DPIA methodology can miss any of these points.

The Article 29 working party recommends EU generic DPIA frameworks from 4 countries (DE, ES, FR, UK) [1] and two EU sector-specific frameworks "Privacy and Data Protection Impact Assessment Framework for RFID Applications" [6] and "Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems" [7]. The ISO/IEC 29134 as international standard is referenced.

For applying our DPIA comparison approach, we will select the DPIA methods from this list. Additionally we will use LINDDUN as the most well-known DPIA framework. We used the following criteria when selecting the methods to compare:

- The method has recently been updated.
- An English version is available.
- The method offers a good selection of supporting material.
- From each of these origin at least one framework is selected: policy-driven, academic, international.

Based on these criteria, the following methods have been selected for detailed description and comparison: LINDDUN, CNIL, ISO/IEC 29134:2017. In the following sections these methods are presented in more detail. Throughout the analysis remarks will be made in the form of numbered notes to underline positive or negative aspects of each method. These will be referenced in the evaluation.

2.2 LINDDUN

LINDDUN is a privacy threat analysis framework, developed by researchers from the DistriNet Research Group at KU Leuven, Belgium [17]. LINDDUN, is an acronym for Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance and consists of 6 main steps.

1. Define Data Flow Diagram (DFD). It uses a data flow diagram to provide a high level graphical description of the whole architecture (based on SDL threat modeling). In a system model there are 4 different building blocks: entity, process, data flow, data store.

Note 1: This representation makes it possible to differentiate between threat analysis (for incoming and outgoing information) and privacy analysis (for internal data flow and processes) which is very helpful. It is also useful to map existing architecture, for example Data store = Data base.

2. Mapping Privacy Threats to DFD. This step helps to identify threats connected to each element in the DFD. Figure 1 shows the LINDDUN mapping table, where each row is a LINDDUN threat category and the columns contain all DFD elements. If a threat is relevant to a DFD type it is marked with X.

Threat categories	E	DF	DS	P
Linkability	X	X	X	X
Identifiability	X	X	X	X
Non-repudiation		X	X	X
Detectability		X	X	X
Disclosure of information		X	X	X
Unawareness	X			
Non-compliance		X	X	X

Fig. 1. Mapping privacy threats to DFD element types (E-entity, DF-data flow, DS-data store, P-process) (Source: [17])

3. Identify Threat Scenarios. Each X in the table has to be examined to determine whether they pose a threat to the system. Lindunn provides a set of privacy threat threes to each X. (With the exception of Disclosure of Information, where LINDDUN points to STRIDE for further analysis). If the threat is relevant misuse cases has to be documented from the misactors point of view. Otherwise the assumptions on why something is not relevant has to be documented.

4. Prioritise Threats. There can be an overwhelming number of threats and due to budget and time limitations first (or only) the most important are considered. Risk assessment is not part of LINDDUN and it offers a number of methods to perform this step: OWASP's Risk Rating Methodology [19], Microsoft's DREAD [20], NIST's Special Publication 800-30 [21], or SEI's OCTAVE [22].

Note 2: It would be useful to have an improved version/combination of these tools tailored for LINDDUN so that the security analyst conducting this step doesn't have to figure out which method would suit his application the best.

5. Elicit Mitigation Strategies. Every threat tree is automatically linked to a mitigation strategy (which later is linked to solution steps). In a case study where LINDDUN was used for DPIA with a Identity Wallet Platform [14] the authors considered this impractical and used the ISO/IEC 27005 *Information Security Risk Management*, which identifies four mitigation strategies: risk reduction, retention, avoidance, and transfer.

6. Select Corresponding Threats. For every mitigation strategy a list of related papers is provided on appropriate privacy enhancing technologies. This is organised as a table and can be found in the supporting materials. In [14] the authors noted that they faced "lack of expertise, low technology readiness level, and other uncertainties regarding the integration of Privacy-Enhancing Technologies (PETs)". They also identified further PETs not present in the table. They also described the need of finding balance between project goals and privacy goals as they had trouble addressing all privacy threats.

2.3 CNIL

The CNIL PIA framework was created by the French data protection authority. They published their DPIA method [3] in November 2018 incorporating the GDPR and the Article 29 Working Party's opinion [1]. It has a very well rounded list of supporting materials: Methodology, Knowledge bases, Templates, Application to IOT devices examples of data processing operations likely to result in a high risk [2] and a software tool that helps to go through the steps [10]. It helps to demonstrate compliance and provides guiding steps to achieve it. Compliance is defined as a combination of the following two pillars: Fundamental Rights and Principles (non-negotiable), Management of data subjects/privacy risks (technical controls). It consists of 4 steps: describe context of processing, guarantee compliance with fundamental principles, assess privacy risks and treat them, and document validation.

1. Study of Context. The main steps here are:

- outline processing
- identify data controller and any processor
- check applicable references: approved codes of conduct (Article 40), certifications regarding data protection (Article 42)
- define personal data concerned / recipients, storage duration
- describe processes and personal data supporting assets.

Note 3: As a first step it doesn't give a good picture of the whole architecture, data movement is not visible and doesn't allow to later differentiate threat analysis and privacy analysis. The online tool doesn't support grouping or any structuring of this information. On the upside it references the GDPR and the relatable sections to help with compliance and clearly defines what is expected at each entry and what the conductor of the DPIA should pay attention to.

Note 4: Article 35(1) requires "a systematic description of the envisaged processing operations". This could be a matter of debate but in contrast to LINDDUN CNIL doesn't fully comply with this point. It does list and describe the processing operations but the process itself doesn't lay out a systematic way on how this should be conducted.

Note 5: Very important to remark: CNIL in its collection of supporting materials among which is a document called "Templates", does provide tables to collect and categorise information. It is not as good as a visual representation but good for record-keeping. However, this paper focuses on the process and the practicality of the DPIA method. If during the steps of the DPIA it is not explicitly mentioned or referenced if something additional is needed for that very step, or the concept is not present in the main document which describes the process, it will not be counted as part of the process. The DPIA should be intuitive with sufficient guidance. Due to the plethora of templates available it is not easy to get a hold of what is needed for a certain step. The main document itself never references to any of the templates and their lack of integration into the process is a serious drawback.

2. Study of Fundamental Principles. The aim is to ensure compliance with privacy protection principles. It consists of two steps: "Assessment of the controls guaranteeing the proportionality and necessity of the processing to enable the persons concerned to exercise their rights" and "Assessment of controls protecting data subjects' rights".

Note 6: This step is a direct translation of the second bare minimum principal from Article 35 (7b) and it is a simple compliance check.

3. Study of Risk. *Note 7*: So far the software tool and the written material were in sync, the tool used the same points described in the text but from this point on it forks into two different processes with different questions.

The document first gives a general introduction to risk assessment with a brief overview on how to calculate risk level. The supporting material *Knowledge Bases* provides a very detailed tutorial on how to determine severity and likelihood with a lot of real life threat scenarios. Study of risks contains two sections. The first one is *Assessment of existing or planned controls* on controls of data being processed: encryption, anonymization etc., general security controls, and organisational controls.

Note 8: The order of the steps so far are incorrect in the documentation. Potential threats were not yet identified neither controls mitigating those threats. Encryption is used if for example confidentiality needs to be protected, but there

are many forms of encryption and first a threat needs to be recognised to use the proper countermeasures.

The second section is on *Risk assessment.* It requires for each impending event:

- determine potential impact on the data subject privacy
- estimate severity of impact
- identify threats to personal data supporting assets, that leads to this feared event (threat scenario) and the risk sources (threat actors)
- estimate likelihood
- determine whether the risks identified in this way can be considered acceptable in view of the existing or planned controls.

Note 9: These steps are out of order. Likelihood and severity has to be calculated before impact.

Note 10: Considering if a risk can be acceptable doesn't qualify as prioritising threats.

The software tool interestingly follows a different steps: Planned or existing measures, illegitimate access to data, unwanted modification of data, data disappearance, and risks overview. It eerily resembles the CIA triad (confidentiality, integrity, availability) with "Planned or existing measures" and "Risk overview" added. It also doesn't categorise the risk properly, neither differentiates between non-negotiable and technical controls.

4. Validation of the DPIA. In a timely fashion this section correspond to Article 35 (7d): "the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance...". It consists of 3 steps: prepare material, formal validation, repeat when necessary (no further comment on how often).

2.4 ISO/IEC 29134:2017

The ISO/IEC standard number 29134:2017 also has a nice selection of supporting material, mainly other ISO standards like a risk-based management system: ISO/IEC 27001, or overview and vocabulary: ISO/IEC 29100:2011 etc. The document itself starts with a long discussion on principles and guidelines related to conducting the DPIA such as: preparing grounds, benefits of DPIA, objectives of reporting, accountability to conduct, scale, determine if DPIA is necessary, preparations, set up a team, prepare a plan, describe what is being assessed, and stakeholder engagement.

The actual steps of the DPIA only starts at Sect. 6.4 and it consists of 5 main steps:

1. Identify information flows of personally identifying information (PII)
2. Analyse the implications of the use cases
3. Determine the relevant privacy safeguarding requirements

4. Assess privacy risks
5. Prepare for treating privacy risks.

The general structure for these steps consists of the following list the conductor has to fill out:
Objective, *Input*, *Expected output*, *Actions*, *Implementation guidelines*.

The guiding document provides a detailed description of what is expected at each point of this list that is tailored to the main steps. After the list it provides a detailed guide with comments and recommendations to further assist the conductor of the DPIA, by for example listing organisational and non-compliance threats and other tips related to that part of the assessment. *Note 14:* This approach makes the whole process a bit monotone almost like filling out a questionnaire but at least it discusses the important topics.

The next sections are the DPIA follow up and the DPIA report. These are more detailed than the DPIA itself. For example the Risk assessment section contains: Threats and their likelihood, Consequences and their level of impact, Risk evaluation, Compliance analysis. But it always references back to previous points so it doesn't mean it was missing from the process. Plus it is easy to put together and provides a very detailed report.

3 Related Work

Although there is an overabundance in available DPIA methods there hasn't been a lot of work on evaluating and comparing them. Further, from the existing literature only a small proportion was published after the GDPR came into force. There are two types of papers in this topic. Evaluating DPIA methods and comparing/measuring the effectiveness of DPIA reports. These are two different fields but in the pursuit of evaluation a lot can be learned from the study of reports as well.

As mentioned before, the GDPR unfortunately does not provide an actual framework to follow and it also doesn't recommend one. This is a shortcoming recognised by Wright et al. already in 2013 [16]. They urged that the European commission and EU member states should draw from the experience of other countries and develop their own DPIA policy, methodology and framework. They also pointed out that a DPIA should be more than a compliance check, as it should be a process. It has to be reviewed and updated throughout the whole life cycle of the project as also stated in Article 35(11). They compared DPIA methods from six countries drawing inspiration from the PIAF project [11] cofounded by the European Commission which reviewed DPIA methods from other countries.

The PIAF delivereable 1 compared the effectiveness of DPIA guides based on a checklist of 18 questions [4, table 10.1] and comparing DPIA reports using checklist of 10 questions [4, table 10.2]. The thirds deliverable [5] outlines what a DPIA process should conatin. These are: Project description, Stakeholder consultation, Risk management, Legal Compliance check, Report, Implementation, Review.

The RFID framework [6] even though it is sector-specific, recognises eight important steps a DPIA should address. These are: characterization of the application, initial analysis, definition of privacy targets, evaluation of degree of protection demand for each privacy target, identification of threats, identification and recommendation of controls, consolidated view of controls, assessment and documentation of residual risks. The frameworks our analysis will focus on are those designed for general use-cases.

So far for comparing DPIA methods the most commonly used technique was to go through a checklist to see if it fulfills certain requirements. However, this can be only done if the evaluation criteria is quantitative in nature and only checks the existence or non existence of a certain aspect. For example in the comparison of Wright et al. one checkpoint is: "Provides a suggested structure for the PIA report". This is a binary question. Whereas other qualitative matters shouldn't be written off with a check-mark. For example points like *DPIA is a process* or *DPIA is more than a compliance check*. It doesn't matter if a method says or claims these points, the real question is how well they fulfill these requirements. It is also pointless to include such questions in a DPIA report analysis as it is not the job of the project owner to invent a working DPIA method that has a nice workflow, rather it's the task of those developing DPIA methods and tools to fulfill these requirements. A report is a statement on what has been performed. These problems are commonly present in previous works by either treating important question as a check-mark and not uncovering shortcomings of the DPIA method, or including questions related to the quality of the method in the report analysis.

An improvement to the check-mark approach was PEGS (PIA Evaluation and Grading System) proposed by Whadwa et al. [15]. Even though this method was developed to evaluate the actual DPIA process post facto (the DPIA report) not the DPIA itself, the authors note that it can be helpful also in guiding a DPIA process. Their evaluation criteria is first presented as a checklist where they provide an extra column where in case a requirements was not fulfilled *scope of improvement* can be specified. Then a weighting is applied in three categories 1, 2 or 3 to each criteria in line with their relative importance, where 1 is the least important and 3 is the most important. Their choice of weights was highly based on the PIAF project. Criteria with weight 1: clarification of early initiation, identification of who conducted the DPIA and publication; weight 2: project description, purpose and relevant contextual information, information flow mapping, legislative compliance checks and identification of stakeholder consultation; weight 3: identification of privacy risks and impacts, identification of solutions/options for risk avoidance and mitigation, and recommendations handling after the PIA.

In a more recent analysis Vemou et al. [13] reviewed 9 different DPIA methods regardless of country of origin with the only criteria that it should not be sector specific, by using 17 questions derived from existing literature as check-marks to draw attention the to lack of completeness of these methods.

4 Comparison of DPIA Methods

4.1 Comparison Metric

To successfully evaluate a DPIA method we should differentiate between three types of criteria. Questions that relate to steps someone should consider prior starting the DPIA are preliminary questions, they are important to consider but they don't have to be integrated into the process. Similarly there are a series of questions only relevant after a DPIA is completed. Like "is publication of the DPIA report provisioned". These are in the territory of DPIA report analysis (which is the scope of our future research) and again is not something that needs to be part of the DPIA process itself. The questions the we focus on are the ones directly related to the steps of DPIA. Questions should also point out the shortcomings identified in the *Notes*. Some questions such as "is it a process" or "is structured guidance to assist in risk assessment provided?" cannot be answered with a single check-mark as they are rather qualitative questions. However, it would be very difficult to build a metric with open questions. In previous works questions related to the DPIA process were simply listed. Here the questions will be structured based on which part of the DPIA process should contain it. It's important to note that Article 29 working party's document is the only official recommendation on how the process should look like. Therefore, we consider that as a starting point[2] .

In total there will be 28 questions. These are categorised based on which part of the DPIA they belong to. The evaluation happens the following way. Each questions will receive grades in two categories: *score* (S) and *process* (P). The Score (S) meant to determine if the question is covered by the method in general. For the score a question can get 0 points if it is not in the method, 1 point if it is partially included, and 2 if its completely addressed. The Process (P) meant to evaluate if a question is well integrated in the DPIA process, for example is discussed in the right part of the DPIA, which can also mean it's part of the method but not placed correctly or logically from the perspective of the whole process. Is it properly discussed with the necessary supporting materials included. For the *process* it can get $+1$ if the step is integrated into the process or -1 if it is not integrated). For a zero Score the Process is automatically zero too. This approach can penalize if a framework while mentioning a certain criterions or questions doesn't integrate its steps into a process and it's closer to a compliance check. For a simple check-mark evaluation this is not possible.

[2] Their "Criteria for acceptable DPIA" checklist, however, is not a blueprint for a good process. The points of Article 35 (7) of the GDPR was also only meant to be a list. Unfortunately, the steps of CNIL is almost a point to point copy of these two.

In this analysis we are not going to focus on a complete compliance checklist but many related questions are included in the process. Checking all the applicable points of the GDPR is not the scope of this paper, as it is more important during the report evaluation.

4.2 Evaluation Questions

This section contains the grading questions split up between six tables for the six steps we identified as crucial parts of the DPIA process. The cells apart from the received grades in some cases also contain a reference to the *"Notes"*. For example *Note 1* is denoted as [(1)]. Grades for (S) and (P) are also separately shown *(Breakdown)* before summarised in the *Total* score where the maximum achievable grade is also shown. Most questions are aiming to evaluate the content of the methods, while others are specifically trying to uncover if the order of steps and questions in the method are designed properly.

Step 1: Description of envisaged processing	ISO		CNIL		LIN.	
	S	P	S	P	S	P
Structured description and mapping of information flows, contextual information and envisaged processing (structured: either graph or table)	2	+1	2	−1 [(3) (4) (5)]	2	+1 [(1)]
Establish easy to follow connections between system elements (data, process, supporting assets etc.)	2	+1	1	−1 [(5)]	2	+1 [(1)]
Allow the differentiation of internal and external data movement	2	+1	0	0	2	+1 [(1)]
Stakeholder identification	2	+1	2	+1	1	+1
Breakdown	8	+4	5	−1	7	+4
Total score (out of 12)	12		4		11	

Both LINDDUN and ISO are using visual representation of the information flows and they are described during the process. LINDDUN is more intuitive but the instructions provided in ISO are more detailed. Unfortunately, the CNIL method really falls behind at this point, which is a very serious issue. This step is the foundation stone for the whole DPIA and missing points here is a serious problem.

Step 2: Assess necessity and proportionality of processing	ISO		CNIL		LIN.	
	S	P	S	P	S	P
How information is to be collected, used, stored, secured and distributed and to whom and how long the data is to be retained	2	+1	2	+1	0	0
Compliance with Article 29 Working party's corresponding list (Annex 2/necessity and proportionality)	2	+1	2	+1	0	0
Analyse all previously identified system elements in a structured manner	2	−1	0 (6)	0 (6)	2	+1
Breakdown	6	+1	4	+2	2	+1
Total score (out of 9)	7		6		3	

LINDDUN is clearly missing assessment steps from a legal perspective and mainly focuses on threat analysis. CNIL does a perfect job from a compliance perspective but it doesn't connect the dots. For the next step we deviate from the suggestion of Article 29 Working Party which would be: "measures envisaged". To determine how the information has to be stored and secured it is important to know the context, from who it has to be protected. Here we prefer the approach of LINDDUN where an early threat analysis is initiated.

Step 3: Identify threats/risks	ISO		CNIL		LIN.	
	S	P	S	P	S	P
Organisational and technical that are endangering the rights of data subjects	2	+1	2	+1	0	0
Origin of risks are specified (threat actor-attack surface)	2	−1	2	−1	2	+1
Threats should be directly linked to elements from step 1	1	−1	1	−1	2	+1
Identification of threats coming from GDPR non-compliance is integrated into the process	2	+1	2	+1	0	0
Threats are identified before Risk Assessment	2	+1	0 (8)	0	2	+1
Is there a differentiation between threat analysis and privacy analysis	2	+1	2	+1	1	−1
Addresses all types of privacy risks (informational, bodily, territorial, locational, communications)	1	+1	1	−1	1	+1
Breakdown	12	+3	10	0	8	+3
Total score (out of 21)	15		10		11	

The ISO standard proves to be the best in this case as well. The drawback of LINDDUN is again the fact that legal compliance is not integrated in the process, which the authors clearly state in the beginning as a result lot of aspects are missing (although some are accidentally tackled). LINDDUN only considers a limited number of threats. CNIL is very strong contentwise but there is no logical structure in its steps and it is a simple compliance check.

Step 4: Risk Assessment	ISO		CNIL		LIN.	
	S	P	S	P	S	P
Structured guidance to assist in risk assessment is provided	2	+1	2	+1	0	0
Fundamental Rights and Principles (non-negotiable) and Management of data subjects/privacy risks (technical controls) are differentiated	1	+1	2	+1	0	0
Risk calculation is included with sufficient supporting material	2	+1	2	−1 [(9)]	0	0
Risks are prioritised	2	+1	1 [(10)]	+1	0	0
Lower risks that are not immediately addressed are well documented	2	+1	1	+1	2	+1
Risk reduction, retention, avoidance, and transfer are all listed as mitigation strategies and sufficiently discussed in supporting material	2	+1	1	+1	0	0
Owner of residual risks specified	2	+1	2	+1	0	0
Breakdown	13	+7	11	+5	2	+1
Total score (out of 21)	20		16		3	

LINDDUN doens't include a risk assessment, only recommends some. It gets some points because in the previous step all threats were already documented. ISO also points out to other ISO/EIC standards and guides, but it does include a structured guide on its own and the recommendations are well referenced and compatible. Whereas LINDDUN leaves the privacy analyst alone to figure out which method would be the best for his use case. If CNILs software tool would be also evaluated for this step its score would be closer or below LINDDUNs.

Step 5: Measures envisaged	ISO		CNIL		LIN.	
	S	P	S	P	S	P
Technical controls and PETs are only discusses after threats and related risks have been evaluated	2	+1	1	−1	2	+1
An extensive list of organisational measures are provided	1	+1	2	−1	0	0
An extensive and updated list of technical measures (PETs) are available	1	−1	2	−1	2	+1
Literature/supporting material for suggested PETs are included	0	0	2	−1	2	+1
Breakdown	4	+1	7	−4	6	+3
Total score (out of 12)	5		3		9	

CNIL again is very vague in the main document but, the fact that in it's "knowledge bases" supporting material provides a wide selection of technical measures none of which is referenced in the process. The list provided by LINDDUN can not be considered complete (neither CNILs or ISO), but it's a step in the right direction.

Step 6: Documentation/Validation	ISO		CNIL		LIN.	
	S	P	S	P	S	P
Outline of the report was generated during the process	2	+1	1	−1	1	−1
Result is evaluated	2	+1	2	+1	0	0
Action plan for continuation	2	+1	2	+1	1	−1
Breakdown	6	+3	5	+1	2	−2
Total score (out of 9)	9		6		0	

Here ISO outruns the other methods in terms of DIPA report preparation. The steps are already outlined in the main document and every step is referenced back to a step from the process.

Evaluation	ISO		CNIL		LIN.	
	S	P	S	P	S	P
Final Breakdown	49	19	42	3	27	10
Final Score (out of 84)	68		45		37	

The overall result shows that, CNIL lost a lot of points for coming off as a compliance check and not trying to be a better process, and due to the lack of references. The ISO method proved to be the best but it could also use a bit if improvement as the order of its steps and the content are good, it feels like

a questionnaire and not a genuine process. LINDDUN needs to develop a step for risk assessment and documentation, while steps and references for GDPR compliance must be incorporated throughout the process.

5 Summary and Outlook

In this paper we performed a comparison of widespread data protection impact assessment methods. By approaching the evaluation and grading from the perspective of a process rather then a compliance check, it became obvious that in many cases very important points of these methodologies are not properly worked out. The ISO standard proved to provide the best framework both contentwise and as a process, although there are still many shortcomings waiting for improvement. The latter is even more true in case of CNIL and LINDDUN. These are among the state of the art DPIA methods with the purpose of: helping companies implementing the Privacy by Design paradigm, support developing GDPR compliance (not least to avoid fines such as Google got), but mostly to assist in the protection of the rights and freedom of natural persons. CNIL has a very good selection of supporting material and in terms of achieving GDPR compliance, it is the best method to go for. However, as a process it really doesn't perform well. LINDDUN has a very good start but it completely misses Risk Assessment and it's 5th step (Eliciting mitigation strategies) is not very intuitive and it's not strong on documentation/validation.

Following Wright et al. [16] we also highlight the importance of one or more officially approved EU-specific DPIA frameworks with sufficient and regularly updated supporting material. In future work we will apply these frameworks to various projects to address the question of GDPR compliance more deeply and analyse the DPIA reports, with the intention of proposing improvements to these methods.

References

1. Article 29 Working Party: Guidelines on Data Protection Impact Assessment (DPIA) (2017). https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
2. Commission Nationale de l'Informatique et des Libertés: Analyse d'impact relative à la protection des données : publication d'une liste des traitements pour lesquels une analyse est requise (2018). https://www.cnil.fr/fr/analyse-dimpact-relative-la-protection-des-donnees-publication-dune-liste-des-traitements-pour
3. Commission Nationale de l'Informatique et des Libertés: Privacy Impact assessment (pia) — CNIL (2019). https://www.cnil.fr/en/privacy-impact-assessment-pia
4. Wright, D., Wadhwa, K., De Hert, P., Kloza, D.: A Privacy Impact Assessment Framework for data protection and privacy rights (2011), https://piafproject.files.wordpress.com/2018/03/piaf_d1_21_sept2011revlogo.pdf
5. De Hert, P., Kloza, D., Wright, D.: Recommendations for a privacy impact assessment framework for the European Union (2012). https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf

6. European Commission: Privacy and Data Protection Impact Assessment Framework for RFID Applications (2011). https://ec.europa.eu/digital-single-market/en/news/privacy-and-data-protection-impact-assessment-framework-rfid-applications
7. European Commission: Smart Grids Task Force (2014). https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force
8. European Parliament & Council: Regulation (EU) 2016/679 - Regulation 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). Official Journal of the European Union L119 (4.5.2016), 1–88 (2016)
9. Quathem, K.V., Tielemans, J., de Meneses, A.O., Shepherd, N.: Google fined EUR 50 million in France for GDPR violation (Jan 2019). https://www.insideprivacy.com/eu-data-protection/google-fined-e50-million-in-france-for-gdpr-violation/
10. de l'Informatique et des Libertés, C.N.: The open source PIA software helps to carry out data protection impact assesment (2019). https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
11. PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights (2011). https://piafproject.wordpress.com
12. Clarke, R.: Roger Clarke's 'Privacy Introduction and Definitions' (2016). http://www.rogerclarke.com/DV/Intro.html
13. Vemou, K., Karyda, M.: An Evaluation Framework for Privacy Impact Assessment Methods. In: MCIS 2018 Proceedings (2018)
14. Veseli, F., Olvera, J.S., Pulls, T., Rannenberg, K.: Engineering privacy by design: lessons from the design and implementation of an identity wallet platform. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing - SAC 2019, pp. 1475–1483. ACM Press, Limassol, Cyprus (2019). http://dl.acm.org/citation.cfm?doid=3297280.3297429
15. Wadhwa, K., Rodrigues, R.: Evaluating privacy impact assessments. Innovation: Eur. J. Social Sci. Res. **26**(1–2), 161–180 (2013). https://doi.org/10.1080/13511610:2013:761748
16. Wright, D., Finn, R., Rodrigues, R.: A comparative analysis of privacy impact assessment in six countries. J. Contemp. Eur. Res. **9**(1), 21 (2013)
17. Wuyts, K., Joosen, W.: LINDDUN privacy threat modeling: a tutorial. CW Reports (2015)
18. Soo, Z.: Alibaba's Jack Ma says he is 'worried' Europe will stifle innovation with too much tech regulation — South China Morning Post (May 2019). https://www.scmp.com/tech/big-tech/article/3010606/alibabas-jack-ma-says-he-worried-europe-will-stifle-innovation-too