Privacy Impact Assessment in Practice

The Results of a Descriptive Field Study in the Netherlands

Jeroen van Puijenbroek
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, the Netherlands
J.vanPuijenbroek@cs.ru.nl

Jaap-Henk Hoepman
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, the Netherlands
jhh@cs.ru.nl

***Abstract*: 'Privacy by design' is not only important from an economic perspective but also from a legal one. The upcoming European General Data Protection Regulation makes privacy by design and default mandatory. One concrete step an organisation can take towards privacy by design is to perform a privacy impact assessment. To verify the assumption that the outcome of the assessment leads to sufficient and adequate input for designing privacy-friendly products and systems that comply with privacy regulations and social norms regarding privacy we performed a descriptive field study in the Netherlands. In this paper, we present the results of this study. Our main results are the following. When performing a privacy impact assessment, organisations use the organisation itself as a focal point, instead of the data subjects whose data is being processed. The proposed countermeasures tend to address the effect rather than the cause of a privacy risk. A consequence of this focus is that the outcome of the privacy impact assessment will lead, at best, to a product or system that is compliant with data protection regulation. It will not lead to a product or system that is privacy-friendly, or one that takes into account social norms regarding the processing of personal information. Another significant result is that the data protection officers who were interviewed perceive the process of determining privacy risks, based on the information gathered about a specific product or system, as vague. Further research is needed to develop a more rigorous and transparent process for determining privacy risks that can be used by organisations.**

Keywords: privacy; privacy impact assessment; privacy by design, General Data Protection Regulation, data protection, data protection impact assessment; data protection by design

I. INTRODUCTION

To build privacy-friendly products and systems that comply with legislation and social norms, privacy [1] needs to be addressed from the very beginning during product or system development. Ex-post implementation of privacy preserving mechanisms into an existing system is in practice very difficult. It mostly involves in-depth system adjustments and is therefore relatively costly. The principle, to take privacy into account throughout the entire development process — from the earliest design stages, through the implementation phase, right until deployment — is called 'privacy by design' [1]. Privacy by design is not only important from an economic perspective but also from a legal one. The upcoming European General Data Protection Regulation [2] (hereafter: the Regulation) which comes into force on 25 May 2018 makes privacy by design and by default mandatory. Organisations need to implement data protection when designing products and services that process personal data. Because of the extra territorial scope of the Regulation this requirement is also important for organisations established outside the European Union when they process personal data of people residing in Europe.

Unfortunately, there are currently no concrete mechanisms that can be used to integrate privacy throughout the entire development process. But such mechanisms are being developed. For example, privacy design strategies have been proposed as a means to translate legal norms into engineering goals that assists to shape a privacy-friendly design during the early stages of system development [3] [4]. Also, the PRIPARE project has proposed a methodology based on best practices, integrating goal-oriented and risk-based approaches [5].

One concrete step an organisation can take towards privacy by design (and actually one that is required for certain types of processing in the upcoming Regulation) is to perform a privacy impact assessment. According to Wright [6] "A privacy impact assessment is a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize the negative impacts". We wish to establish whether the outcome of the privacy impact assessment leads to sufficient and adequate input for designing privacy-friendly products and systems that comply with privacy regulations and social norms regarding privacy. To verify whether this is indeed the case we performed a descriptive field study between late 2015 and mid 2016 in the Netherlands.

In this paper, we present the results of this field study regarding the use of privacy impact assessments in practice, and compare this to the theory and the requirements stipulated in the upcoming Regulation (Section V). For our study, we selected fourteen organisations across eight sectors with different data subject categories and different sizes. We interviewed the data protection officers of these organisations using a predefined survey. Our methodology is explained in Section IV.

The main answer (see section VI for details and

[1] In this paper, we focus on safeguarding personal data processing. We have chosen the term "privacy" rather than "data protection" because of the broader scope. See section II

substantiation) to our research question is that the outcome of the privacy impact assessment for most of the interviewed organisation will lead, at best, to a product or system that is compliant with data protection regulation. It will not lead to a product or system that is *privacy-friendly*, or one that takes into account social norms regarding the processing of personal information. We conclude this paper with suggestions for further research on this topic (see section VII).

II. Data protection or privacy

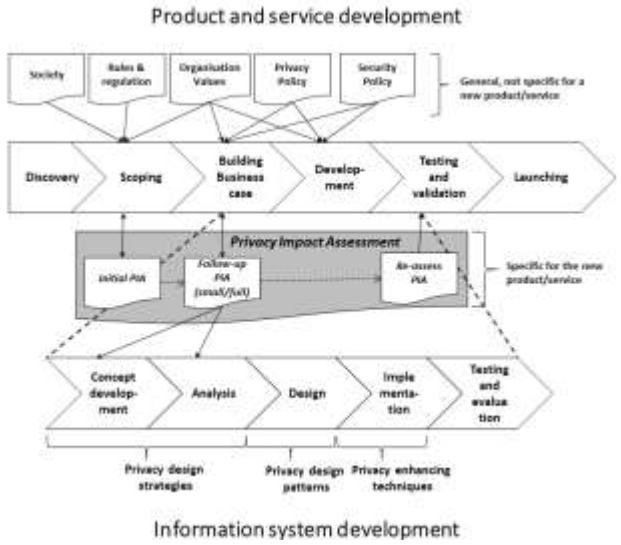
In this paper, we do not only take the legal requirements on data protection into account, but also the social norms (values/expectations) regarding the processing of personal data. This broadening of the scope is prompted by Wright's definition of privacy impact assessments and the concerning article in the Regulation which mentions that (representatives) of the data subject (the person about whom personal data is processed) can be consulted during such a privacy impact assessment. Also, this approach is inspired by the fact that non-compliance with societal values may lead to significant negative publicity. For example, in the Netherlands social indignation arose in 2014 when Equens (a payment service provider) launched the idea to sell the payment transaction information of customers. The same occurred in 2014 when ING Bank wanted to do a pilot in which it would offer personalised third-party ads to their customers (with their consent) based on their individual spending patterns. Both ideas were formally compliant with the Dutch Data Protection Act.

Because we not only take into account the legal requirements regarding data protection but also social norms and expectations we use the terms privacy impact assessment and privacy by design instead of the terms used in the Regulation such as 'data protection impact assessment' and 'data protection by design'.

III. Privacy by Design and Privacy Impact Assessments

Privacy by design is intended to improve overall privacy friendliness when designing an information system. The fundamental principle of privacy by design is that privacy requirements must be taken into account throughout the entire system development process. Privacy is a core property of a system that is heavily influenced by the underlying system design. As a consequence, privacy by design cannot be implemented as an add-on [3]. Traditionally, privacy by design is linked to the system development process. We believe, however, that the 'cradle to grave' philosophy of privacy by design means we should not start thinking about privacy in the first phases of the *system development* process, but in fact already in the initial phase of the *product development* process. After all, the development of an information system is not a goal in itself but supports a product or a service. When, for instance, the outcome of the initial privacy impact assessment, as part of the scoping phase of product development, is taken into account when building the business case an informed decision can be made. Therefore, the privacy impact assessment can and should provide input for both development processes, which blend into each other. For a graphical representation of our positioning of the privacy impact assessment see Fig. 1. In this paper, we concentrate on the influence of privacy impact assessment on information system development.

Fig. 1. Privacy impact assessment (PIA) in relation to product and system development



As mentioned earlier a privacy impact assessment is a process for assessing the impacts on privacy of a product or service, and for taking remedial actions as necessary in order to avoid or minimize negative impacts. These remedial actions *can be* [2] taken into account when implementing technical and organisational measures to ensure a level of protection appropriate to the risks of infringement on the rights and freedoms of natural persons. Roughly one can distinguish the following three phases in a privacy impact assessment: 1) collect the necessary information, 2) determine privacy risks and 3) propose mitigating measures to avoid or reduce the determined privacy risks. The outcome is normally documented in a report. That report can be used both as input for the concept development and analysis phase of the system development lifecycle, as well as for the testing and evaluation phase of that cycle. The use of the report in the latter phases helps to determine if the countermeasures ultimately chosen during the implementation phase have indeed eliminated or mitigated the initial identified privacy risks. We did not assess the quality of the outcome of the privacy impact assessment.

IV. Research Methodology

We performed a descriptive field study in the Netherlands among fourteen organisations between late 2015 and mid 2016. The selected organisations are distributed across eight sectors (see Table I) with different data subject categories (e.g. consumer, passenger, patient, civilian) and different sizes of organisations. In this way, we gave preference to a wide variety of sectors above the ability to compare results per sector.

[2] One of the amendments of the European Parliament on the proposal for the Regulation was that the output of the privacy impact assessment *needs to be* taken into account. This amendment has not been adopted in the final version of the Regulation. The final text of the Regulation merely mentions that a privacy impact assessment *needs* to be conducted where the type of processing is likely to result in high privacy risk.

TABLE I. DISTRIBUTION SELECTED ORGANISATIONS OVER SECTORS

Sectors[3]		Number of selected organisations
Section	***Description***	
C	Manufacturing	2
J	Information and communication	2
H	Transport and Storage	2
K	Financial and insurance activities	1
M	Professional, scientific and technical activities	1
N	Administrative and support service activities	1
O	Public administration and defence	3
Q	Human Health and social work activities	2

We interviewed the data protection officers (or someone with an equivalent role) of each of the fourteen organisations using a predefined survey. We did not question or discuss the answer (to prevent bias), apart from asking for clarification when the answer was not clear.

At the time of the interviews the Data Protection Directive [7] was still in force and implemented in the Netherlands through the Dutch Data Protection Act [8]. Under that legislation, the conduction of a privacy impact assessment is only obliged for some types of processing of personal data by public authorities. The European General Data Protection Regulation was not finalised yet. Only the proposal [9], the position paper and amendments of the European Parliament [10] and the position paper of the European Council [11] were published.

TABLE II. SURVEY QUESTIONS

A.	***Why and when to conduct a PIA***
	1. How do you define PIA? Has the definition been published?
	2. Why do you conduct a PIA?
	3. Since when has your organisation conducted PIAs?
	4. How many PIA's are conducted in your organisation?
B.	***How to conduct a PIA***
	1. Can you describe how a typical privacy impact assessment is initiated and executed within your organisation?
	2. In which cases does your organisation conduct / not conduct a PIA (is there a threshold)?
	3. Is there a guideline how to conduct a PIA? On which methodology or standard is it based?
	4. Has the PIA been built into the project management of another business process?
	5. Who conducts the PIA (an individual or a team, which functions are represented)?
	6. In which phase or phases in the product and/or information system development is the PIA conducted?
	7. Is there one questionnaire for all data processes or is it tailor made (e.g. depending on the development phase or depending on standard or tailored software)?
C.	***How to determine privacy risk and measures***
	1. How do you define privacy risk?
	2. How are privacy risks determined/identified in a PIA (automatically/manually)?
	3. How does your organisation cope with reducing privacy risk (strategy)?
D.	***Results from the PIA (PIA and PbD)***
	1. How do you determine that the output of the PIA is used for concept development and analysis (information system development)? i) If the output is used, how is guaranteed that the results of the PIA are known and used by the IT-department? ii) If not why? What do you need?
	2. How and when is monitored if the mitigating measures of PIA are implemented during the development phases?
	3. Did the outcome of the PIA resulted in changes in the (specs of the) information system.
E.	***Consultation with stakeholders***
	1. Who are the stakeholders?
	2. Are the results of the PIA consulted with stakeholders? Which stakeholders? If not, why not?
F.	***Governance PIA***
	1. Is the quality of the PIA assessed? By whom?
	2. Is somebody assigned to manage the PIAs (e.g. the privacy officer)
	3. Are PIAs periodically revised (is this an obligation)?

Table 2 describes the questions used during the interviews to verify our assumption that the outcome of the privacy impact assessment should lead to sufficient and adequate input for designing privacy-friendly products and systems that comply with privacy regulations and social norms. This is why, it is in our opinion necessary to get insight into why organisations conduct privacy impact assessments, what their definition of privacy risk is, what their strategies of reducing privacy risk are, when and how the assessments are conducted, whether the organisation scales the assessment (small/full) depending on the phase of development and/or the type of data processing, who the stakeholders are, and how the quality is assured. We also wanted to gain insight into how organisations use the output of the privacy impact assessment for privacy by design.

V. RESEARCH RESULTS

In this section, we present and discuss the outcome of our survey. We do this treating for each of the six topics separately. For each topic, we first present a summary of the responses for each of the questions that belong to that topic. We then follow through with our analysis of that topic: we compare the outcome of our interviews with the theory (especially the work of Wright and De Hert [6] [12] [13] [14]), our own expectations and the relevant articles and recitals of the Regulation. The latter to determine what the selected organisations need to take to "migrate" from the current practice to the practice they have to comply with in the near future.

A. Why and when to conduct a privacy impact assessment

1) Questions and answers

- *How does your organisation define a privacy impact assessment? Has the definition been published?* Most organisations defined the privacy impact assessment as a tool/process to determine whether there are privacy risks, how big they are and to provide recommendations for mitigating measures. According to these organisations, the definition used was described briefly in the privacy impact assessment-documentation. In a few cases the privacy impact

[3] The section and description of each sector is taken from the International Standard Industrial Classification (ISIC) of the United Nations [18]

assessments were an integral part of the system development process and were not treated and thus not documented separately.

- *Why does your organisation conduct a privacy impact assessment?* Most organisations conducted a privacy impact assessment because they thought it was mandatory for them. In a few cases it was mentioned that the assessment was conducted to prevent the loss of customer trust or to prevent an inappropriate infringement on the personal life of the customer.
- *Since when has your organisation conducted privacy impact assessments?* Most of the organisations started conducting privacy impact assessments in 2012-2013, some in 2006-2010 and one organisation as early as 2002.
- *How many privacy impact assessments are conducted in your organisation?* Most organisations had no (central) database with all conducted privacy impact assessments and had to make an estimation. The amount varied from 15 to 550. Most organisations only conducted privacy impact assessments on new or revised systems. Others also conducted the assessments on existing systems because they did not do it in the past and now wanted to have insight into the privacy risks the organisation could face.

2) Main findings - Why and when to conduct a privacy impact assessment

Under the current data protection legislation most of the selected organisations, except for governmental authorities under certain circumstances, are not obliged to conduct a privacy impact assessment. Nevertheless, most data privacy officers mentioned that it is mandatory. This obligation can be stipulated in the Binding Corporate Rules[4] or other Group policy rule that some of the organisations have implemented. Others wrongly perceived it as an obligation. Although a privacy impact assessment should be more than simply a compliance check, it does nevertheless enable an organisation to demonstrate its compliance with privacy legislation in the context of a subsequent complaint, privacy audit or compliance investigation. A privacy impact assessment enhances informed decision-making and exposes internal communication gaps or hidden assumptions about the project [6].

Because there was no real obligations to conduct privacy impact assessments for most of the selected organisations we expected that data protection officers would mention reasons for conducting the assessment spotting potential privacy problems and taking effective countermeasures (early warning), avoidance of inadequate solutions, avoidance of negative public reaction or loss of trust and reputation, avoidance of unnecessary costs or education, raising awareness about privacy among employees or gaining competitive advantage [14]. This was not the case, however.

Under the upcoming Regulation conducting a privacy impact assessment will be mandatory, dependent on the nature of the processing. For processing likely to result in a high risk to the rights and freedom of natural persons organisations have to carry out the assessment. The Regulation stipulates that the assessment shall in particular be required in the case of a) automated processing (including profiling) on which decisions are based that produce legal effects concerning natural persons; b) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; and c) a systematic monitoring of publicly accessible area on a large scale (art. 35 par. 3 GDPR).

B. How to conduct a privacy impact assessment

1) Questions and answers

- *Can you describe how a typical privacy impact assessment is initiated and executed within your organisation?* Almost all organisations executed the privacy impact assessment more or less the same way. They started by gathering the necessary information for the assessment (mostly through a questionnaire). Based on that information the privacy risks were determined and mitigating measures were proposed to and agreed to be implemented. Within some organisations the residual privacy risks that remain because not all measures were implemented must be approved by senior management.
- *In which cases does your organisation conduct / not conduct a privacy impact assessment (is there a threshold)?* Most organisations conducted the privacy impact assessment for *each* system in which personal data was processed: there was no real threshold. Some organisations used the amount of financial investment for the new/changed information system as threshold to determine whether a privacy impact assessment was needed, for example investments worth over 1 million euros. Some other organisations performed a pre-scan, which provided a preliminary determination whether a privacy impact assessment was required.
- *Is there a guideline for how to conduct a privacy impact assessment? On which methodology or standard is it based?* Most organisations had some kind of guideline or framework for conducting privacy impact assessments. There was no uniformity at this point. For governmental authorities the "Framework privacy impact assessment Dutch National Government" [15] was required in case of new or revised legislation that results in the collection or processing of personal data, and for large IT projects. Some organisations used the privacy impact assessment framework of the NOREA [16] (the professional association for IT auditors in the Netherlands). Some used the frameworks (incl. questionnaires) of the law firms that helped them with implementing Binding Corporate Rules and others developed their own framework.
- *Has the privacy impact assessment been build into the project management of another business process?*

[4] 'Binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity (art. 4 par. 20 GDPR).

Almost all organisations said that the privacy impact assessment was part of a larger assessment. In order of occurrence (from many to few) the privacy impact assessment was part of: compliance, project delivery, information security and business impact assessment. The credo of one of the data protection officers is "to burden the organisation as little as possible by 'free-riding' on existing procedures".

- *Who conducts the privacy impact assessment (an individual or a team; which functions are represented)?* More than half of the organisations conducted the privacy impact assessment through several bilateral consultations between the data protection officer/privacy advisor and other officers of that organisations (business owner, senior staff, analyst (business/infra), information security officer, lawyer, etc. The remaining organisations conducted the assessment with a team of which the data protection officers/privacy advisor is a (supporting) team member. The size of the team depended on the project, and typically consisted of the aforementioned other officers of the organisation. In some organisations there was a strict separation between the monitor compliance-task and the advisory-task of the data protection officer. The data protection officer monitored compliance and the privacy advisor advised. When a privacy advisor was appointed, he or she participated in the privacy impact assessment and the data protection officer revised it.
- *In which phase or phases in the product and/or information system development is the privacy impact assessment conducted?* Almost all data protection officers mentioned that they *intend* to conduct the privacy impact assessment in the early phases of system development. The problem was that it was not always common practice for project managers to consult the data protection officer about a new project. Within some organisations, it was a requirement that the privacy impact assessment had been conducted before the development could continue (this was part of a gateway review). Although it could take several meetings to complete a privacy impact assessment, it was not a dynamic process for these organisations. It was conducted in a specific moment (phase), not over a period of time. A few organisations followed a process oriented approach, where they started during product development and supplemented the assessment during the system development.
- *Is there one questionnaire for all data processing or is it tailor-made (e.g. depending on the development phase or depending on standard or tailored software)?* Almost all organisations used one questionnaire for all phases and for all types of personal data or data subjects. Some organisations used different types of frameworks depending the kind of data processed and thus different questionnaires. One organisation used a master privacy impact assessment for the repetitive part of projects and used an addition privacy impact assessment for the unique parts of the projects. None of the organisations had different questionnaires depending on whether the product/service would be supported by standard software or tailored software.

2) Main findings – How to conduct a privacy impact assessment

Most of the data protection officers of the selected organisations conduct privacy impact assessments in more or less the same way and for all processing with one questionnaire. The assessment is, with a few exceptions, conducted early in the development process. The threshold to conduct an assessment or nor is the question whether personal data is processed or not. This is not appropriate. First, the degree of risk created by projects varies enormously. Second, projects vary widely – from updating a small database to implementing new legislation, or developing a new product or service. Some authors recommend that organisations conduct a limited preliminary evaluation, to establish whether the organisation needs to invest in a small-scale or a full-scale privacy impact assessment [17]. The scalability of the assessment and thus questionnaire should in our opinion also depend on the phase of the development process. Up front, we expected that different questionnaires would be used in different phases of development or that the questionnaire had separate sections for the different phases. This is required to steer the process. An "initial" privacy impact assessment would be conducted during product development and the first phase of system development (concept development) to determine if the project is even viable taking privacy risks into account. During the development process the initial privacy impact assessment could then be supplemented with a 'follow-up' version.

All selected organisations check at the end of the development process (test and evaluation) whether the agreed upon measures are indeed implemented. In that phase, the data protection officers do not re-assess the privacy impact assessment. Privacy risks could have changed or new risks may appear as a result of design and/or implementation decisions. A re-assessment should therefore be carried out. (See Fig. 1 for a graphical representation for the relationship between these three types of privacy impact assessments and the other product and system development phases). However, as mentioned earlier, Wright states that the privacy impact assessment should be regarded and carried out as a process and not just as a single task that results in the completion of a report [14]. Based on our interviews we conclude that this process-oriented approach needs further improvement in organisations.

An organisation should determine the roles and responsibilities of its officers with regard to privacy impact assessment, for example who initiates one, who carries it out and who approves them. A team of experts, including external ones, might be necessary. The privacy expertise is crucial here but it does not exclude other fields. Outsourcing the privacy impact assessment in full is not desirable. The line manager should be responsible for conducting the assessment because, first and foremost, she is accountable for the risks posed by her products/services. Secondly, she knows the product/service well and hence should be able to tell where the main risks are. Finally, doing a privacy impact assessment internally would help to create privacy awareness throughout the organisation [14]. In our opinion these reasons also favour the team based approach

over of the bilateral approach. In the latter, there is a risk that the line manager no longer feels accountable anymore for the privacy risks posed by her products/services. The data protection officer faces the risk that accountability is shifted towards him. This is clearly undesirable. (Line) management is responsible and the data protection officers provides advice where requested as regard to the privacy impact assessment and monitors its performance pursuant the requirements mentioned in the Article 35 GDPR.

C. How to determine privacy risks and measures

1) Questions and answers

- *How do you define privacy risk?* In most cases privacy risk was defined from the perspective of the controller, i.e. unlawful processing of personal data resulting in high fines of the Supervisor Authority and loss of reputation. In a few cases the risk was perceived primarily from the perspective of the data subject, e.g. infringement on the personal life of the data subject, resulting in loss of trust of the customer which could cause loss of market share. In these cases possible fines were only secondary.
- *How are privacy risks determined/identified in a privacy impact assessment (automatically/ manually)?* Within almost all organisations the privacy risks were determined manually (mostly supported by the data protection officer/privacy advisor). A few organisations used a mechanism which determined possible risks and mitigating measures automatically. The organisations that used privacy advisors mentioned that the quality of the determined the privacy risks was very dependent on the skills and experience of the person determining that risk. The data protection officers who were interviewed perceive the process of deriving privacy risks based on the filled-out questionnaire as vague. One of the data protection officers compared it to a black-box.
- *How does your organisation cope with reducing privacy risk (strategy)?* Most data protection officers mentioned that their organisation did not had a general strategy for reducing privacy risks. When asked to give examples of solutions to reduce the privacy risk, the organisations that defined the privacy risk from the perspective of the controller tended to favour measures that mitigate the risk (e.g. encryption or access management) instead of avoiding risks (e.g. pseudonymisation or data minimisation).

2) Main findings - How to determine privacy risks and measures

In the Regulation "data protection risk (privacy risk)" is not defined. The corresponding article about privacy impact assessment only mentions "…the rights and freedoms of natural persons…". This indicates that, from the point of view of the Regulation, the data subject perspective is more relevant than the controller perspective. The process of determining risks and measures is not well defined, and no guidance is provided. As a result, the quality of it very much depends on the person performing the privacy impact assessment. It is a black box. In addition, solutions to reduce the privacy risk are sought in measures mitigating the risk instead of avoiding the risk; especially in organisations that define privacy risk from the perspective of the controller. This is understandable (but not defendable). When the data protection officer defines privacy risk as the risk of getting fined by the Supervisory Authority he will look at the effect of a privacy risk instead of the cause. When you subsequently determine measures to reduce the privacy risk –bearing in mind the effect of the privacy risk– you are more likely to start thinking in terms of measures to reduce the risk of non-compliance. When you determine measures – bearing in mind the cause of the privacy risk– you probably start thinking in measures that reduce the inherent risk, i.e. the cause. This does not mean that in all cases the ultimately chosen solution will be sought in avoiding privacy risks. See Fig. 2 for a graphical representation.

Focussing on the risk to the controller will lead at best to products or systems that are compliant with data protection regulation, but the resulting system may not always be privacy-friendly.

Fig. 2. Layers of privacy risk

D. Results privacy impact assessment

1) Questions and answers

- *How do you establish that the output of the privacy impact assessment is used for concept development and analysis (information system development)? If the output is used, how is guaranteed that the results of the privacy impact assessment are known and used by the IT department? If not why? What do you need?* Most organisations (in the person of the project owner, data protection officer, information security officer, executive management, etc.) agreed to implement the measures proposed in the privacy impact assessment. In the organisations where information security officer was involved the data protection officers believed that the measures were more likely to be developed. The project owner was ultimately responsible for implementing the agreed measures.
- *How and when do you monitor whether the mitigating measures of privacy impact assessment are implemented during the development phases?* As part of the information system design cycle the developed system was tested to determine whether it is built in conformance with the specifications (including the

ones from the privacy impact assessment). The test team gave a "go/no go". Sometimes the project owner must sign off explicitly that the measures of the privacy impact assessment had been implemented; otherwise the project would be placed on hold.

- *Did the outcome of the privacy impact assessment result in changes in the (specifications of the) information system.* As a result of the privacy impact assessments personal data was better secured, in some cases less personal data was collected and in other less personal data was presented (e.g. on screens and letters). Besides the specific improvements in information systems, conducting privacy impact assessments resulted in enhancing awareness of data protection throughout the organisation.

2) Main findings - Results from the privacy impact assessment

As part of the information system design cycle the developed system is tested to verify that it was built in conformance with its specifications. As mentioned earlier, the data protection officers should re-assess the privacy impact assessment during the 'testing and validation'-phase because privacy risks could have changed or new risks may appear as a result of design and/or implementation decisions.

E. Consultation with stakeholders

1) Questions and answers

- *Who are the stakeholders?* The data protection officers mentioned departments/ officers within the organisation as stakeholders. The ultimate stakeholder, the data subject was hardly mentioned. Only when the data processing involved personnel, the working counsel was mentioned as stakeholder.
- *Are the results of the privacy impact assessment consulted with stakeholders? Which stakeholders? If not, why not?* The results of the privacy impact assessment were only shared with the involved officers within the organisation; not everyone within the organisation had access to (a subset of) the report. None of the selected organisation published (a subset of) the privacy impact assessment report externally. Only one case involved data subjects. This organisation involved customers for improving the quality/friendliness of the consent notice in an UX-lab to achieve a higher consent rate of their customers as legal grounds for processing personal data.

2) Main findings - Consultation

The data subject is one of the stakeholders of the privacy impact assessment-process whose remarks must be taken into account [6]. Even the selected organisations that use customer panels for judging new products/services did not seek consultation with the customer or their representatives about their perceived privacy risk, and which mitigating measures are or are not acceptable. Based on the Regulation, the controller shall, where appropriate, seek the views of the data subject or their representatives on the intended processing.

F. Governance privacy impact assessment

1) Questions and answers

- *Is the quality of the privacy impact assessment assessed? By whom?* The quality of the privacy impact assessment was secured through the participation of experts in the team. If privacy advisors were used the data protection officer typically reviewed it. In some organisations, the report was signed off by key parties (like applicable line manager, data protection officer, information security officer and depending on the residual risks also executive management). This not only improved the involvement of the key parties but also the quality of the report. Little or no auditing of the privacy impact assessment was performed.
- *Is somebody assigned to manage the privacy impact assessments?* Among the selected organisations there was no common understanding. The following people were mentioned as being responsible: the product owner, the data protection officer, the chief information officer, risk management department.
- *Are privacy impact assessments periodically revised (and is this an obligation)?* About half of the organisations did not specify conditions for revising a privacy impact assessment. The other organisations had explicit conditions for reassessment of the impact of privacy risks (every two to three years, or earlier in case of large changes). In one case the revision of the privacy impact assessment was part of a certification program for that information system (5 years).

2) Main findings – Governance privacy impact assessment

As seen earlier, in most organisations the roles and responsibilities involved in conducting privacy impact assessments are described. But managing the life cycle of the privacy impact assessment is not. At best a revision term is specified. This needs to be improved.

VI. CONCLUSIONS

We conducted a field study regarding the use of privacy impact assessments in practice in the Netherlands. The main results of our study are the following:

- Most of the data protection officers who were interviewed perceive wrongly that they are obliged to conduct a privacy impact assessment. The European Data Protection Directive (which was in force at the time we performed our study) does not mention such an obligation at all. The upcoming European General Data Protection Regulation stipulates that only in circumstances where the processing is likely to result in high risks to the rights and freedoms of natural persons does an assessment need to be carried out.
- Most organisations use an uniform approach (incl. *one* questionnaire) for assessing all data processing, regardless of the type of processing and the type of project. Based on existing research a preliminary evaluation was expected to determine whether to conduct a small-scale or full-scale privacy impact assessment.

- Most organisations conduct the privacy impact assessment at one phase during system development (in the early phases) but they do not supplement the assessment during the development process. Existing research states that the assessment should be regarded as a process, and not just as a single task.
- Most data protection officers define privacy risks from the perspective of the controller (the risk of getting fined by the Supervisory Authority) instead of the perspective of the data subjects. This is not in accordance with the spirit and the legal requirements specified in the Regulation.
- When reducing the assessed privacy risks most organisations favour measures that mitigate risks, instead of measures that avoid them.
- Most organisations do not consult (representatives of) the data subjects as part of the privacy impact assessment process. Consultation is advised by a number of authors [6] [14] [17], and the Regulations also stipulates that "where appropriate, the controller shall seek the views of the data subjects or their representatives on the intended processing".
- The process of determining privacy risks, based on the information gathered about a specific product or system, is perceived as vague and its quality is very dependent on the person who assesses the privacy impact assessment.

Most of the participating organisations were highly controller-oriented instead of data subject-oriented when considering privacy risks. This was apparent from the reasons for conducting privacy impact assessments and the definitions of privacy risk given by the data protection officers, the proposed measures for reducing the privacy risk, and the practice of not consulting (representatives of) the data subject as stakeholders. These organisations tend to look at the effect rather than the cause of a privacy risk. When the outcome of a privacy impact assessment by these highly controller-oriented organisations is used to implement the principles of 'privacy by design', this will lead at best to a product or system that is compliant with data protection regulation. It will not lead to a privacy-friendly product or system and/or one that takes into account social norms regarding privacy.

VII. Next steps, further research

A more rigorous and transparent process for determining privacy risks that can be used by organisations in practice needs to be developed. Data subject risks, instead of controller risks, should be central. And these risks should be avoided instead of merely being mitigated: the output of a privacy impact assessment should steer the initial system design. In fact we believe the privacy impact assessment process and the resulting privacy by design process should be integrated into a single methodology (what we call a Privacy Impact Reduction Methodology) that fosters the development of truly privacy-friendly products and systems that, by default, comply with both data protection regulations and social norms.

References

`

[1] A. Cavoukian, "Privacy by design," Office of the Information and Privacy Commissioner of Ontario (IPC), Ontario, 2009.

[2] EC, "Regulation (EU) 2016/679 of the European Parlement and of the Counsil on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (L119/1)," vol. L119/1, 2016.

[3] J.-H. Hoepman, "Privacy Design Strategies," *IFIP SEC,* pp. 446-459, 2014.

[4] M. Colesky, J.-H. Hoepman and C. Hillen, "A Critical Analysis of Privacy Design Strategies," 2016.

[5] N. Notario, A. Crespo, Y.-S. Martín, J. M. d. Alamo, D. L. Métayer, T. Antignac, A. Kung, I. Kroener and D. Wright, "PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology," in *IEEE CS Security and Privacy Workshops*, 2015.

[6] D. Wright, "The State of the art in privacy impact assessment," *Computer Law & Security review,* vol. 28, pp. 54-61, 2012.

[7] EC, "Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data," vol. L281:31.

[8] DP, "Ducth Data Protection Act (Transl. Wet bescherming persoonsgegevens)," *Dutch Official Gazette,* vol. 302, 2000.

[9] EC, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data," vol. COM(2012)11, 2012.

[10] EC, "EP legislative resolution of 12 March 2014 on the proposal for a regulation of the EP and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)," vol. P7_TA(2014)0212.

[11] EC, "Position of the Council of 19 December 2014 on the proposal for a regulation of the EP and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data," vol. Doc.15395/14.

[12] D. Wright, K. Wadhwa, P. D. Hert and D. Kloza, "A Privacy Impact Assessment Framework for data protection and privacy rights - Deliverable D1," Brussels, 2011.

[13] G. Hosein and S. Davies, "A Privacy Impact Assessment Framework for data protection and privacy rights - Deliverable D2 (Empirical research of contextual factors)," Brussels, 2012.

[14] P. d. Hert, K. Daiusz and D. Wright, "Recommendations for a privacy impact assessment framework for the European Union - Deliverable D3," Brussel, London, 2012.

[15] Rijksdienst, „Framework privacy impact assessment Dutch National Government (Transl.Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst)," juni 2013.

[16] NOREA, "Priacy Impact Assessment; Introduction, Guidance and Questionnaire (Transl. Privacy Impact Assessment; Introductie, handreiking en vragenlijst)," 2015.

[17] A. Warren, R. Bayley, C. Bennett, A. Charlesworth, R. Clarke and C. Oppenheim, "Privacy Impact Assessments: International experience," *Computer Law& Security Report,* vol. 24, pp. 233-242, 2008.

[18] UN, "International Standard Industrial Classification of All Economic Activities (ISIC), Rev. 4," United Nations Publication, New York, 2008.