Privanova

Risk & Compliance

YOUR ONE-STOP SHOP GDPR COMPLIANCE PROVIDER

PRIVACY IMPACT ASSESSMENTS FOR H2020 PROJECTS

Sharing ideas and best practices

26/12/2019

CONTACT

privanova.com

contact@privanova.com

linkedin.com/company/privanova

TABLE OF CONTENT

Part I - Introduction

Context

Performing a Privacy Impact Assessment on an innovative ICT project is an essential part of a wider, proactive, risk-based approach to privacy and data protection.

Often, publicly funded Research & Development projects such as those financed by the EU Commission within the former FP7 or the current H2020 framework involve consortia consisting of large number of partners.

If foreseen, the task of ensuring compliance with privacy and data protection regulation is usually dedicated to one consortium partner that is responsible for the design and implementation of a privacy strategy.

In order to adequately manage privacy and data protection risks in a proactive way, this strategy should, at least, include an initial Privacy Impact Assessment (PIA).

Ideally, a single team of assessors performs every aspect of the PIA. This, however, is neither practical nor always possible for big consortiums involving multiple partners.

Based on their specific expertise and capabilities, partners share the workload, and are responsible for different aspects of the project. As a consequence, the team performing the PIA might not have the time, knowledge or other means necessary to preform an in-depth PIA for each and every aspect of the project under the responsibility of different consortium partners.

This is why, in order to understand different contexts in which each consortium partner operates, the team of assessors often has to create and send out a PIA questionnaire, relying on their partners to provide adequate information and eventually identify and evaluate privacy related risks on their own.

This approach is based on the assumption that each consortium partner has the necessary means to understand the context in which personal data is processed within the scope of the project under its responsibility, and that because of this, the consortium partner in question is in better position than the PIA team to identify and evaluate risks and to provide solutions to avoid or to reduce these risks.

The role of the assessor here is to design PIA documentation and coordinate its implementation with other partners. However, this approach has several obstacles that may hamper the efforts of the PIA team:

- Consortium partners do not have sufficient legal, technical, or other skills necessary to successfully execute their part of PIA (such as providing sufficiently well argumented, true answers to PIA questionnaire);
- Consortium partners are reluctant to preform a PIA because it is viewed as somebody else's responsibility;
- Consortium partners are reluctant to preform a PIA because it would disclose the lack of their regard for privacy and data protection, or the lack of internal privacy policies and safeguarding mechanisms;
- Instead of providing high-quality, detailed answers that are the result of a collaborative effort from people with different responsibilities (legal, IT, etc.) to the PIA questionnaire, consortium partners forward the questionnaire to one person who fills it out and sends it back just to get rid of it.
- Consortium partners do not understand the importance of PIA, and privacy and data protection in general.

Purpose of this document

This document is by no means intended to be a comprehensive guide to PIA.

Written in a hope that bits of information it contains might be useful in avoiding possible pitfalls of performing a PIA on a multidisciplinary R&D project involving multiple partners with different competences and privacy practices, its purpose is to share some of our experiences and ideas with potential assessors who find themselves in a similar situation.

Structure

This document contains four sections. The introduction is followed by a discussion providing some general suggestions that might be applied to any PIA performed in a similar context.

After preliminary questions, the design and the content of the PIA questionnaire and other documentation are discussed. The need to draft documents in such a way that persons without legal background can easily understand and act upon them is stressed.

Finally, the big picture is addressed, placing the PIA in a wider context of a proactive, hands-on approach to privacy & data protection risk management. Here, suggestions about other means of maximising the effects of the PIA such as awareness rising activities are outlined.

Part II - Before you start

Prepare the ground

When performing a PIA on a project-wide scale, the team of assessors may encounter issues even before the design phase of a project-specific privacy strategy and the appropriate PIA questionnaire. For example, these issues might arise from the fact that:

Project documentation (DOW, Consortium Agreement, etc.) does not expressly use the term “Privacy Impact Assessment”. This may result in difficulties when trying to convince other consortium partners of the necessity to perform a PIA.

Consortium partner responsible for project-wide privacy strategy is “only” one among equals, and its request for a PIA may be interpreted as an obligation unilaterally imposed on other partners who do not understand its nature.

Consortium includes partners (i.e. SMEs, private labs etc.) who do not have adequate expertise necessary to interpret legal or technical aspects of the PIA questionnaire.

With these examples in view, and before going into the actual design of the PIA questionnaire and its supporting documentation, the team of assessors may find beneficial to address the following questions.

Get support from the project leader

In order to perform a high quality PIA, the team of assessors must gather information from other project participants and communicate with them on a regular basis.

However, the consortium partner responsible for implementing PIA is typically one among several project participants, with more or less equal status. This is why, in order to provide more authority and weight to its requests, the PIA team should seek clear, open support from project leader in advance.

This is especially true for big consortia, where the project leader plays the role of coordinator, and may influence project participants and act as a bridge between them.

Consequently, during the design phase of the privacy strategy, the consortium partner responsible for privacy strategy should convince the project leader of the importance and the necessity of performing a PIA on a project-wide scale, and get his support.

At a later stage, when other consortium partners need to be informed about their role in performing the PIA, from a purely practical point of view, co-signing emails and other documentation by both the assessor and the project leader is one of the most effective ways of providing more authority to requests sent out to other partners.

Effective arguments supporting the idea of having a project-wide privacy strategy based on PIA are many. Benefits of the proactive approach range from legal compliance to risk management, and from building consumer trust and good reputation to gaining a competitive edge on the market. The privacy team should pick the most important ones, adapt them to the context of the project and use them to support their views.

The most challenging task, however, is not only to try to find an effective set of arguments answering the question “why do we need a PIA”, but also to effectively communicate these arguments to other partners so they can be understood, adopted and acted upon. The narrative must be adapted to the audience in order to produce the maximum effect.

Involve the relevant people

PIA is not the domain exclusively of law specialists. Innovative ICT projects involve many disciplines and require multidisciplinary approach. In some cases team of assessors will need to seek advice and information from other partners, and vice-versa: provide information from their field of expertise.

In an ideal situation, a PIA should be part of the project governance system. However, this is often not the case, and the related tasks are the sole responsibility of only one partner, even if the overall responsibility for the correct implementation of the privacy strategy is shared between all project participants. In this situation, it is important to include in PIA process persons in position to provide correct information and implement PIA results (usually project managers). They should own a part of the responsibility for the overall PIA success.

Always provide guidance and assistance

Providing guidance and assistance to other project partners is one of the key elements for successful conclusion of a PIA. As stated before, partners may or may not have enough knowledge and resources to complete PIA on their own. This is why it is important that the team of assessors be as much available as possible to provide any information that will enable other partners to go forward with the PIA.

Being present and helpful is especially important during the “questionnaire” phase of the PIA when project partners need to provide clear answers about their specific context in which the personal data are being processed.

Documenting everything

Documenting everything is important for several reasons.

Firstly, documenting PIA process is important for ensuring transparency and accountability in the project. This is especially significant during the “questionnaire” phase of the PIA, when team of assessors must guide other partners and help them in providing good, correct information about the context in which personal data are being processed. All requests for assistance or information alongside with the answers provided must be documented. Since it is very probable that several project participants may ask similar questions, documenting what was already answered will also save time.

Secondly, when PIA is completed, a full report should be submitted and communicated to other project partners. The report, or its summary might be made publicly available and used in different ways. In some cases the submission of this report to DPA is required.

Often, big R&D projects carry the need to withhold some information from the public. This commonly includes information related to intellectual property, and issues concerning defence, law enforcement, financial interests etc. This is why, generally, only PIA summaries are made publicly available. A balance between legal limitations to publication and the principle of transparency and accountability in the project should be achieved.

Part III - Drafting the PIA Questionnaire & Supporting Information

Communicating legal concepts

As stated before, one of the main challenges is to create a PIA questionnaire specifically tailored for the project. However, this is not enough.

Consortium partners may be very different from one another. Not only they may have different fields of expertise (IT, social sciences, etc.), but can also be very diverse in size (SMEs or large multinational entities), and in nature (public universities or private companies). Internally, different partners may have different privacy and data protection policies and practices already in place. Finally, in case of EU-funded R&D projects, consortia must include partners from different countries, meaning different legal systems as well.

These issues render the design of an effective PIA questionnaire very difficult. On top of that, for the PIA procedure as a whole to be successfully executed, it is necessary that all the involved partners have the same understanding of the language used in the questionnaire, and employ the same set of legal and technical terms.

Faced with these issues, that team of assessors should create not only a project-specific PIA questionnaire, but also accompany this questionnaire with additional information helping their partners to understand PIA's nature, content and purpose.

Persons who do not necessarily have legal background, and probably come from different countries must easily understand this information. In order to be effective, this document should provide concrete examples.

Supporting Information

The approach to PIA that results in compliance "checklist" should be avoided as much as

possible. This is why it is a good idea to include the PIA questionnaire within a more comprehensive document containing information necessary to ensure that project partners clearly understand:

- Their obligation to provide truthful information;
- Main goals of the privacy strategy in general, and PIA in particular
- Legal as well as technical terms used within the document;
- What are the next steps, and what is expected from them.

Legal base

Brief overview of the legal norms on which the obligation to perform a PIA is based is often useful to avoid any doubts project partners may have in this regard. The necessity to provide correct answers and to collaborate with the PIA team should be logically explained and derive from these norms.

Explaining the "what" and "why"

This part of the document should address questions such as:

Short operational definition of a privacy impact assessment. Often it is best to approach this from risk management point of view, as people are often familiar with this concept.

General benefits of the proactive, Privacy by Design approach. In several paragraphs, provide arguments in favour of PbD approach that are relevant for the project. It might be a good idea to explicitly state what are the situations we want to avoid by relying on PbD, and what are the intended results of this approach. Giving real life examples helps.

Need for multidisciplinary collaboration. The necessity for all partners to collaborate on the implementation of the privacy strategy and PIA should be clearly explained. Partners should know that they can rely on support from the PIA team in completing the questionnaire. In return, they must also expect further inquiries from the PIA team in case more technical information is needed to identify and evaluate privacy and data protection risks. Finally, multidisciplinary

collaboration is needed in order to find adequate solutions for avoiding or reducing identified privacy risks.

Defining core concepts

This part of the document should provide list of definitions concerning legal, technical and other terms used in the questionnaire and the supporting documentation.

Legal definitions should be followed by real-life examples that describe for instance the meaning of "personal data", "processing of data", "data transfer" etc. within the scope of the project. The examples must be related to the project, mean something for the participants, and help them understand underlying legal concepts and their importance.

Having the same vocabulary is of the utmost importance for project where participants come from different countries (with different legal systems, traditions and practices).

Stating the Objectives

Objectives specific to the PIA should be explained here. This part of the supporting documentation should list project-specific goals, corresponding potential risks and give examples of real-life situations in which these risks might arise.

Its purpose is to help project partners understand "what is a privacy risk" and what is expected from them when replying to the questionnaire. In our experience, this greatly improves the quality of replies as well as decreases partner's demand for assistance during this phase of the project.

For this part of the document, a list of "Generic privacy targets and concrete sub targets" from Oetzel and Spiekermann's article on Privacy by Design can be a good starting point (**Oetzel, Marie Caroline, and Spiekermann, Sarah**: *Privacy-by-design through systematic privacy impact assessment – a design science approach*, ECIS 2012, Barcelona, 2012).

Examples should be provided with relation to the project in order to be aligned with the context in which PIA is performed.

Structuring the questionnaire

In case project partners are not only asked to provide replies to the questionnaire, but to identify as well as to evaluate privacy risks, the structure of the PIA document as well as the main phases should be explained. This means that, from the Phase 1 (providing information about the context), which mostly relies on the questionnaire, Phases 2 on risk identification, 3 on risk evaluation and eventually Phase 4 on solutions must be addressed.

Even superficial understanding of the main PIA phases helps project partners to provide better answers to the questionnaire as well as to have a general overview of the steps that follow.

In case they are requested to go thru Phases 2-4 and to identify, evaluate and address identified risks by providing concrete solutions, they should be informed about the significance of these phases and be reassured that help is available if they need it.

Part IV – Moving forward

PIA Report

The findings arising from the PIA and recommendations for mitigating risks are consolidated into a PIA report.

Publication of PIA report and its content should not come as a surprise to other project partners. This is why it might be a good idea to submit the Report as a draft first, and seek input from all participants. The quality of PIA report can be enhanced if the participants have the opportunity to challenge PIA team on their findings, or further explain their point of view. This does not mean that the independence of the PIA team should be compromised. In any case, all partners share the responsibility for ensuring privacy within the scope of the project.

PIA report has its value as both internal compliance and risk management tool for consortium partners and external, "public-facing" tool for PR, awareness raising etc.

Training and Awareness Raising Activities

PIA is only one element of a sound PbD strategy. It should be complemented by awareness campaigns and training of all kinds. Even if assessments are conducted, there is a lot of work to do in implementing the findings.

Keeping up awareness about privacy is a challenging task. However, awareness-raising activities are necessary because they facilitate the implementation of the privacy strategy in general and recommendations for mitigating risks in particular.

Furthermore, since big R&D projects often cover a period of several years it is natural to provide training to project participants. This training may target specific people on key positions, or be oriented towards all involved. Training in form of an interactive, hands-on workshop may prove effective, especially in a multidisciplinary context. The main goal of the training is to enable project managers to influence their subordinates so that important decisions are not taken without taking privacy into account.

PRIVANOVA

Risk & Compliance