DP Impact Assessment: A technologist's perspective

Dr. Rehab Alnemr suggests an automated tool for conducting PIAs, a process that is soon to be mandatory for high-risk processing.

In November 2007, the UK Data Protection Authority, the Information Commissioner's Office (ICO) launched a privacy impact process to help organisations assess the impact of their operations on personal privacy. This process assesses the privacy requirements of new and existing systems; it is primarily intended for use in public sector risk management, but is increasingly seen to be of value to private sector businesses that process personal data.

The ICO's latest guidance was published in 2014: Conducting privacy impact assessments code of practice[1].

The newly agreed EU General Data Protection Regulation (GDPR) requires business operating in the EU to undertake data protection impact assessments (DPIAs) which are a broader version of privacy impact assessments when dealing with projects that handle personal data. Articles 32a and 33 provide the conditions under which a DPIA would be mandatory[2]. The goal of DPIAs is to identify the main risks of a project with respect to the rights and freedom of data subjects concerning their personal data. DPIA can be a safeguard of privacy and data protection rights as it requires companies to systematically consider the intended data processing, and the associated privacy risks and the measures to be taken to mitigate these risks, especially for privacy intrusive projects and services.

The GDPR also gives examples of risky projects where conducting a DPIA is important, such as processing activities that use health information, race, large scale surveillance, personal data about children or biometric data. A DPIA needs to address the intended purpose of data processing and the necessity and proportionality of that processing, while taking into account the entire lifecycle management of personal data from collection to processing to deletion.

Why it should be automated?

In practice, a DPIA screening consists of a set of questions which helps to assess the risks for personal data involved in the intended processing. The DPIA process can be carried out manually by a Data Protection Officer (DPO) or a privacy specialist. The problem is that they need to do so for every single project that process some kind of personal data in their company, which is very time consuming and may leave regular employees with a significant lack of knowledge in this area, since someone else is doing the data protection checks for them without educating them on its practice. If the organization is a Small and Medium Enterprise (SME) rather than a big company, they may not have the resources to assign a privacy specialist to check on the risks involved in every project. Automation of the process, in the form of a DPIA tool, will enhance an organization's overall risk management practice and contribute towards raising employees' awareness regarding data protection and governance. A DP officer can then revise the final reports produced by the tool and give recommendations accordingly.

> We have created a DPIA tool automating the process of identifying the risks.

How can it be done?

In the Accountability for Cloud (A4Cloud)[3] EU Project, we have created a DPIA tool automating the process of identifying the risks related to a certain project but also identifying the risks of using certain cloud service providers. It is a systematic process to:

- elicit threats to the privacy of individuals,
- identify the procedures and practices in place to mitigate these threats, and
- document how the risks were addressed in order to minimize harm to users.

The tool reports on two categories of risks: one related to the project itself and the other related to the cloud provider. The first category is concerned with risks to data sensitivity, compliance with regulations, cross-border data transfer as well as risks related to data transparency, control, security, and sharing. The second one calculates risks based on the security controls used by the cloud provider. The risk assessment process itself is automated and based on an algorithm that we have developed to give the user a report regarding the aforementioned risks. The resulting report can also act as evidence used by DPOs to prove that the company is performing the necessary steps to comply with the regulations and general accountability practices. Each question has several possible suggested answers avoiding open questions, which are hard to process automatically, and an explanation about the meaning of the question itself. While answering some questions the user can get guidance from the tool on how to address the privacy issues highlighted by the specific answers given. If a company is developing a similar tool for their future DPIA process, a mechanism needs to be developed to review and update the legal content of the tool at appropriate intervals to ensure that it does not become dangerously inaccurate.

A multidisciplinary approach is the key

The approach used in building the final questionnaire in the DPIA tool is based on legal and socio-economic analysis of privacy issues for cloud deployments, building on the expertise of experts from different disciplines in legal research, information security and risk management, and user experience design. The goal was to create a set of questions that cover information about: the type of project being assessed, how data is collected and used, how it is stored and what security measures are in place, transfer of information to third parties or cross-border, and finally cloud specific questions. Having such an approach, of bringing together experts from different fields, helped us bridge the gap between legal requirements and technologists' understanding of these requirements.

We used several resources to develop the questionnaire such as the Data Protection Directive[4], the GDPR draft, the ICO's PIA Handbook, and some PIAs models from other countries. The EU DP Directive provided us with the basic concepts and principles defining the current general data protection framework, while the GDPR provided additional concepts and concrete procedural guidelines for a practical DPIA questionnaire.

User experience and awareness also essential

Many privacy impact assessments models work on the assumption that the user is aware of certain basic data protection notions, such as 'personal data' and directly ask the user whether they process personal data and for which purposes and on what ground and so forth. In our questionnaire, we start from the premise that the user does not know these concepts and it therefore tries to, within limits, do a legal qualification of the user's responses to simple terms. Based on the kind of information the user intends to process, the tool will decide that it constitutes personal data, rather than having the user specify so in advance. The tool does provide feedback incorporating proper legal terminology where applicable. This is one of the tool's goals of raising awareness of data protection practices. We accomplish this goal by using a user centric design, facilitating understanding and educating users about privacy risks, but also by simplifying the legal language used in the questionnaire without compromising the intended meaning. We have gone through several iterative processes to reduce the number of questions to 50, having experienced that users will be overwhelmed by more than that threshold.

Recommendations

The questionnaire developed in the A4Cloud Project, of course, does not capture the whole of the relevant laws and regulations that are far too complex, lengthy, and granular to be represented in a tool. However, the aim is to ease a soon-to-be mandatory process by the GDPR, allowing DPOs to perform more efficiently, and make it a standard practice in companies while educating employees in the process. Companies must start to instill in place a well-defined data protection impact assessment process that will not overwhelm their DP Officers and at the same time help educate their employees in data protection practices. In order to do so, they need the help of both the legal and the technology sides of the company so they can reach a middle ground, where the process is neither too complicated with a legal language that cannot be understood or followed by their employees, nor it is completely automated with no legal checks from the DPOs or privacy offices. Ways to mitigate perceived risks identified by the DPIA process need to be agreed upon by both technologists and legal personnel in the company.

QUESTIONS AND ANSWERS ON THE DP IMPACT ASSESSMENT TOOL

PL&B: You write: "The DPIA questionnaire will be published soon on the A4Cloud website." When will the tool be published on the A4Cloud website? When do you expect to publish the DPIA questionnaire?
Rehab Alnemr: The implementation of the tool will not be available but the questionnaire, which enables anyone to create the tool, will be published on our project's website by the end of March 2016 and will be available for free.

PL&B: What is HP's business model on this service, for example, free trial for a certain period then payment one off or on a monthly basis? How much will it cost?
Rehab Alnemr: HP provides and operates cloud services for our customers. Our interest here is to ensure that it is easy and effective for ourselves and for our customers and suppliers to perform these impact assessments. That is why we are making the questionnaire publicly available. Customers and suppliers could integrate the impact assessment questionnaire with their own business risk assessment processes and tools.

PL&B: What are the practical aspects of use, for example, whether this tool is intended for PCs, Apple computers, and/or other systems?
Rehab Alnemr: The tool is a web based tool so it is platform independent. The idea is that anyone can take the questionnaire and use it as a basis to build their own tool.

PL&B: Will you seek ICO certification of this tool?
Rehab Alnemr: Since it is a prototype and it belongs to the EU project, no plans for certification have been made.

• For project enquiries, contact: Julie Grady Julie.grady@hpe.com

AUTHOR

Dr. Rehab Alnemr is an R&D Engineer at Hewlett Packard Labs.
Email: r.alnemr@me.com

REFERENCES

1 https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/ and click on Privacy by Design and then on the pdf titled Conducting privacy impact assessments code of practice (2014)
2 High risk for the rights and freedoms of individuals.
3 Cloud Accountability Project (A4Cloud) www.a4cloud.eu
4 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 on the free movement of such data OJ L281/31 (DPD) (1995).

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

6. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business Reports*. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work. **Steve Wright, Chief Privacy Officer, Unilever**"

Subscription Fees

Single User Access
UK Edition **£400 + VAT***
International Edition **£500 + VAT***
UK & International Combined Edition **£800 + VAT***
* VAT only applies to UK based subscribers

Multi User Access
Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts
Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.
Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):
Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30
Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the International Report.
www.privacylaws.com/int