CLOUD ACCOUNTABILITY PROJECT

Data Protection Impact Assessment:

A questionnaire to support cloud customers evaluate data protection risks in the cloud

Project Release

This document has been edited by Rehab Alnemr (HPE).

Contributors to this document include Rehab Alnemr (HPE), Siani Pearson (HPE), Dimitra Stefanatou (Tilburg University), Lorenzo Dalla Corte (Tilburg University), Alexander Garaga (SAP), Anderson Santana De Oliveira (SAP), Asma Vranaki (QMUL), Niamh Gleeson (QMUL), Amy Holcroft (HPE), Massimo Felici (HPE).

This work has been partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no:317550 (A4CLOUD) Cloud Accountability Project.

Data Protection Impact Assessment:

A questionnaire to support cloud customers evaluate data protection risks in the cloud

CLOUD ACCOUNTABILITY PROJECT

SEVENTH FRAMEWORK PROGRAMME

Why DPIA?

Data protection impact assessment (DPIA) is used to assess potential harm to individuals as well as the risks to carrying out processes. Organizations will have to carry out a DPIA once the new EU General Data Protection Regulation (GDPR) is in effect.

What is the DPIA questionnaire?

This is a questionnaire that can be used in the DPIA process. It facilitates and supports the DPIA process by creating a consistent artefact that can be used by organization to assess privacy and security risks in their projects.

It is a set of 50 questions – and associated explanation – based upon analysis of the EU Data Protection Directive (DPD), and the proposed EU GPDR.

What does it cover?

Six areas: the type of the project, collection and usage of the information, storage, security, transfer of information, and (where appropriate) cloud-specific questions.

How can it be used?

It can be used as a guideline to what to ask during a DPIA process or as the bases for a DPIA tool.

Automating the process

We have created a prototype tool using this questionnaire: Data Protection Impact Assessment Tool (DPIAT) for organisations to identify and highlight what the privacy and security risks are for a given configuration and environment, as well as for any proposed usage of a cloud provider. The tool educates the users about these risks, and thereby can be used to reduce risk and demonstrate due diligence when selecting service providers or developing products and services.

Further information

- EU 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 (General Data Protection Regulation), 2012.
- Rehab Alnemr, et. al. “A Data Protection Impact Assessment Methodology for Cloud”, in the Proceedings of the Annual Privacy Forum, Springer LNCS, 2015.

ID	Question	Explanation
Type of Project		
1	Is the establishment of your activities in European territory?	Whether the processing of personal information of your undertaking takes place in the European Union or not is not relevant. If you are not established in European Union territory, but you offer goods or services to individuals in the EU or monitor them, then you should answer Y to this question.
2	Do you handle information that can identify other people through one or more of the following activities?	Think for instance, if you use names, identification numbers or location data. The collection of information related to individuals can be potentially intrusive to the information privacy rights of these individuals. In some types of projects information provided is more sensitive than in other ones e.g. Financial data.
3	For which of the following purposes or legitimate interests do you process the information?	To be legitimate, the processing of information should be based on legitimate interests. Some interests carry more weight than others. For instance processing for historical, scientific statistical or research purposes is likely to be less intrusive to information privacy rights e than processing for exercise of the right to freedom of expression or information.

ID	Question	Explanation
Collection and Use of Information		
4	Are you relying exclusively on consent in order to process information of individuals?	Consent means 'any freely given specific, informed and explicit indication of his or her wishes by which the individual either by a statement or by a clear affirmative action signifies agreement to information relating to them being processed.'
5	How have you obtained the consent of individuals?	Consent requires prior information and an explicit indication of the intent to consent.
6	If individuals have given their consent, can they withdraw it with ease and whenever they want to?	Individuals should be able to withdraw their consent at any time and every step of the processing of their information without detriment. It should be as easy to withdraw consent as it is to give it.
7	Are the consequences of withdrawal of consent significant for individuals?	For instance, will the service to the individual be terminated, while the individual depends on it?
8	On what basis do you process the information?	In order for the processing to be lawful, at least one of these grounds must be satisfied.
9	Do you provide clear information about:	

ID	Question	Explanation
10	Are all the information and its subsets you handle necessary to fulfill the purposes of your project?	The information you collect/process/handle should be adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed. This means that you have to use the minimum information necessary for your purposes, but you are not prohibited to have multiple purposes.
11	Is it possible for the individual to restrict the purposes for which you process the information?	For instance, are individuals given the possibility to opt-out of receiving email offers from you?
12	Is the nature of your operations such that you need to comply with rules regarding data processing in more than one set of regulations?	Think for instance specific (data protection) regulation pertaining to you, such as for financial or health services.
13	Are decisions being made on the basis of the information you process?	For instance, information can be collected for historical purposes without being used as part of a decision process.
14	Do the outcomes of these decisions have a direct effect on the individuals whose information is processed?	For instance, are offers based on the characteristics of individuals being collected by your system?

ID	Question	Explanation
15	Does the information you process about individuals produce a full and correct image of these individuals?	The chances of taking wrong decisions increase if the information is incomplete, outdated or wrong. In such cases, the risk of setting individuals' rights at stake is higher.
16	Does the information you process about the individual come from different sources?	Think, for instance, whether you obtain databases from other parties
17	Are the individuals whose information you process aware of the fact that the information comes from different sources?	Consider whether you have informed the individuals about the information you process and which might come from other sources.
18	Does your project involve the use of existing personal information for new purposes?	For instance, you may decide that you want to use the contact details you obtained for signaling the user that their order has been fulfilled for marketing purposes later on.
19	Do your additional processing operations relate closely to the original purposes for which you first collected the information?	For instance, using a customer's home address for frequent delivery of packages after the first delivery is compatible use, whereas providing a patient list to one spouse, who runs a travel agency; so that he can offer special holiday deals to patients needing recuperation is not.

ID	Question	Explanation
20	Is the use of existing personal information for new purposes clearly communicated to the individual in a timely manner?	Consider whether you have informed the individuals about the specific (new) purposes for which you process the information
21	Is the use of existing personal information for new purposes clearly communicated to your organization's data protection officer?	Consider whether you have informed the data protection officer about the specific (new) purposes for which you process the information.
22	Is the use of existing personal information for purposes not previously notified clearly communicated to the Data protection authority?	Consider whether you have informed the Data protection authority about the specific (new) purposes for which you process the information.
23	Do you process information which could potentially be perceived as discriminatory?	Think for instance, whether you process information solely on the basis of race or ethnic origin, political opinion, religion or beliefs, trade union membership, sexual orientation or gender identity etc.
24	Are procedures in place to provide individuals access to information about themselves?	Consider, for instance, whether individuals can request an overview of the information about them that you have
25	Can the information you process be corrected by the individuals, or can individuals ask for correction of the information?	An increased level of involvement by the individual decreases the likelihood of unwarranted events (e.g. incorrect information)

ID	Question	Explanation
26	Do you check the accuracy and completeness of information on entry?	Consider, for instance, whether you apply specific procedures (e.g. use of journalistic archives to double-check the content) in order to ensure the validity and authenticity of the information you process.
27	How often the personal information you process is updated?	Outdated information has a negative impact on the accuracy of information you process.
28	How severe would you deem the consequences, in case you process outdated information for the individuals it refers to?	For instance, having outdated information about individuals (e.g. wrong date of birth) may hold you liable.
29	Would the fact that the information you process is not up to date lead to sanctions provided in relevant regulations?	Think, for instance, whether the nature of your activities requires you to comply with specific sets of regulations, which provide sanctions in order to keep the information updated.
30	Do you have a Data Security Policy?	Think of aspects such as: is it clear who is responsible for security, do you adopt security standards, is the (sensitive) nature of the information you process taken into account.

ID	Question	Explanation
31	Do you implement any technical and organizational security measures from the outset of your activities?	Think, for instance, whether you are using signatures, hashes, encryption etc. or whether you implement Privacy by Design and/or Privacy by Default mechanisms.
32	Do you differentiate your security measures according to the type of information that you process?	For instance information related to race or ethnic origin, political or sexual orientation, religion or gender identity of the individuals requires specific security measures.
33	Are your personnel trained on how to process the information you deal with according to the organisational policies you implemented?	Consider if you apply specific procedures or timetables to train your employees with regard to the manner in which they should process the information.
34	How often are your Security and Privacy Policies updated?	
35	Do you adopt one or more of the following measures and/or procedures as a safeguard or security measure to ensure the protection of personal information?	The application of one or more of the following measures may prevent potential misuse of the information you handle.

ID	Question	Explanation
36	If you use encryption methods, are you responsible for encrypting and decrypting the information that you process?	If you are the only one responsible for encrypting and decrypting the information you process, you are subsequently the only one who has control over this information. Instead, if you have given such a competence to a cloud service provider you do not have the same level of control over the information.
37	Do the protection measures you have in place, in case of unwarranted incidents, specifically target the particular type of incident that might happen?	For instance, in case of unauthorized access/ disclosure/modification, intentional or reckless destruction of or damage to your equipment, loss or theft of your assets etc. Such incidents threaten the protection of personal information.
38	Do you take action in order to notify individuals in case of (security) incidents?	E.g. by sending emails.
39	What do you do to minimize the damages of physical, technical and/or security incidents?	
40	Does the project(s) include the possibility by individuals to set retention periods on their own?	Setting retention periods allows you to ensure that the information that you process about individuals is kept for no longer than is necessary for your operations.

ID	Question	Explanation
41	For how long do you store the information you are dealing with?	
Transfer of Information		
42	Do you transfer the information you deal with to third parties?	Do you, for instance, outsource the processing of the information you deal with to third parties?
43	Is the third parties' use compatible with the one you set for your undertaking?	If you transfer information to third parties, they use the information in a manner consistent with your purpose(s) and their mandate.
44	Do you sell, rent or by any means disseminate information to third parties?	
45	Are you transferring and/or simply disclosing personal information to a country or territory outside of the EEA?	The EEA consists of the following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxemburg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.

ID	Question	Explanation
46	Are you transferring personal information **exclusively** to one or more of the following non-EEA countries?	Each of these countries are deemed to have adequate privacy protection in terms of the EU data protection regulations.
47	Are measures in place to ensure an adequate level of security when the information is transferred outside of the EEA?	Not all countries have the same level of protection as regards to the processing of personal information.
Cloud Specific Questions		
48	The cloud infrastructure (hardware and/or software) I use is:	The potential threats to privacy and protection of personal information are influenced by the deployment model of the CSP. This means that the risk is higher if the number of the subjects who operate in the system is also high.
49	Does the service that you use consist of the provision of end user applications run by the cloud service provider?	Think for instance of SalesForce CRM or Wuala.
50	Are specific arrangements in place with regards to your information in case you want to terminate or transfer the cloud service?	The application of such rules/procedures gives you the ability to have control/access over the information you process. For instance, you can transfer the information you process to another provider if needs be (bankruptcy, force majeure etc).

Contributors

This research was carried out within the context of the Cloud Accountability Project (A4Cloud). This project is developing methods and tools, through which cloud stakeholders can be made accountable for the privacy and confidentiality of information held in the cloud.

For more information

- EU Cloud Accountability (A4Cloud) Project: http://www.a4cloud.eu
- info@a4cloud.eu.

This project is partly funded from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4CLOUD).