CLOUD
ACCOUNTABILITY
PROJECT

Data Protection Impact Assessment:

Supporting cloud customers in evaluating 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.

Why DPIA?

Data protection impact assessment (DPIA) is used to assess potential harm to individuals as well as the risks to carrying out processes. There are strong requirements emerging relating to the need to measure the impact of business on privacy, within the revised European data protection regulation. Based on this regulation, running a data protection impact assessment is going to be mandatory for organisations in certain situations. Organisations will have to carry out a DPIA once the new EU General Data Protection Regulation (GPDR)[1] is in effect. The A4Cloud project has produced a questionnaire and recommendations to help in the data protection assessment process. It was tailored to satisfy the needs of Small and Medium Enterprises (SMEs) that intend to process personal data in the cloud.

What is the DPIA questionnaire?

This is a set of 50 questions 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 organisations to assess privacy and security risks in their projects. The questionnaire is based on a legal and socio-economic analysis of privacy issues for cloud deployments including analysis of the EU Data Protection Directive (DPD)[2], the proposed EU GPDR, the UK Information Commissioner's Office's (ICO) PIA Handbook[3], and the PIA Guide of the Office of the Australian Information Commissioner (OAIC)[4]. The questionnaire does not assume that the user is familiar with certain basic data processing notions such as 'personal data' but rather helps the user in identifying whether personal data is being processed. It also considers the protection of data subjects as the core of its assessment.

What does it cover?

The questionnaire covers six areas: the type of the project; collection and usage of the information; storage; security policies; data transfer; and (if appropriate) cloud-specific questions. The aim of this set of questions is to assess how the interactions between the organisations that perform the DPIA and cloud service providers (CSPs) affect data subjects' rights to privacy and data protection.

How can it be used?

The questionnaire can be used as a guideline about what to ask during a DPIA process or as the basis for an automated DPIA tool.

---

[1] COM 11 final 2012/0011 (COD) European Commission: 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 (General Data Protection Regulation). Brussels, 25.1.2012 p. 1. (2012)

[2] 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)

[3] Information Commissioner's Office: Privacy Impact Assessment Handbook, http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf (2011)

[4] Australian Government, Office of the Australian Information Commissioner: Privacy Impact Assessment Guide (OAIC) (2010)

Questionnaire explained

Each question in the questionnaire has the following elements:

- **Identity (ID)**: A reference to the question and its associated information.
- **Question**: The text that will be asked to the user of the DPIA.
- **Explanation**: Text explaining the question itself.
- **Question Type**: The type of options that each question has as an answer i.e. a Yes/No answer, multiple choices, one choice of many, etc.
- **Response Yes/No**: The text displayed in case of answering yes or no which will explain the implication of this particular answer or further information regarding this answer.
- **Action on Yes/ No**: The answer to some of the questions can lead you to skip some of the following questions, this attribute indicates which question to follow based on the given answer.
- **Score**: The privacy impact score based on the answers. These scores will be used later to calculate the final risks scores.
- **Weight**: The weight prioritising the importance relative to other questions.
- **Privacy Indicator**: Most questions have one or more indicators capturing different privacy aspects.

Scores

The evaluation that is the result of the DPIA is based on the scores associated with each question. Each question has a formula for computing the privacy impact score based on its answer and a weight prioritising the importance relative to other questions. For example, Question 4 in the questionnaire "*Are you relying exclusively on consent in order to process information of individuals?*" has the following possible answers:

a) Consent is given directly by the individual by a statement (e.g. by a consent form)

b) Consent is given directly by the individual by an affirmative action (e.g. by ticking a box)

c) Consent has been obtained implicitly by the individual (e.g. by merely use of the service or inactivity)

We assign the value for the *privacy impact score* for the answer to this question using the following formula: *If option 'a' then the score is 0, Else if option 'b' then the score is 1/4, Else if option 'c' then the score is ¾.*

Intuitively, option 'c' would have a bigger impact on privacy than option 'b' and 'a' so the score is chosen to be proportional to the perceived impact. In addition, we associate the questions with several *privacy indicators*, capturing different privacy aspects: *data sensitivity*, *compliance*, *trans-border data flow*, *transparency*, *data control*, *security*, and *data sharing*. For example, the answer to the question above influences the *data control* and *transparency* indicators. Some of the indicators can enhance privacy (*compliance, transparency*, *data control* and *security*), while the others diminish it (*data sensitivity, trans-border data flow and data sharing*). Therefore, the privacy indicator scores will be either proportional to the privacy impact scores of individual answers or inverse. So in the example above a higher score for the answer (option 'c') implies less data control and transparency.

We compute the *final privacy indicator score* for the indicator *j* (e.g. Sensitivity) is: $I_j = \frac{\sum_i s_i \times w_i \times \alpha_i \times \beta_{ij}}{\sum_i w_i \times \alpha_i \times \beta_{ij}}$, where β_{ij}=1 if the answer to question i impacts indicator j and β_{ij}= 0 otherwise. $\alpha_i = 1$ if question i is answered and $\alpha_i = 0$ otherwise. $s'_i = s_i$ if the indicator j negatively affects privacy and $s'_i = 1 - s_i$ otherwise. There is inverted semantics for indicators that diminish security such as *data sensitivity, trans-border data flow, and data sharing*. w_i is the weight associated with question i.

Finally, we define the overall *privacy impact level* and *privacy indicator levels* for the assessment by translating the score to a uniform qualitative scale: *Low* < *Medium* < *High* and use color-coding to facilitate the presentation: *Low* → Green, *Medium* → Yellow and *High* → Red.

Privacy risk indicators

There are seven privacy indicators:

Sensitivity (SEN): Risks related to a sensitive market (i.e. elderly, children, etc.) and/or sensitive data (i.e. health or medical conditions, finance, sexual behavior)

Compliance (C): Risks related to compliance with external standards, policies, laws, etc.

Trans-border data flow (TB): Risks related to transfer of information across national borders

Transparency (T): Risks related to transparency in the areas of notice/user messaging and choice/consent

Data control (DC): Risks related to control of the data lifecycle (i.e., collection, usage, quality, and/or retention)

Security (SEC): Risks related to security of data and data flows

Data sharing (DS): Risks related to sharing data with third parties

A broader data protection impact assessment process

This questionnaire is meant as an initial building block on which to base your future assessments of how your projects and activities could potentially impact individuals' rights to privacy and data protection, and all the other rights that are connected to them. A Data Protection Impact Assessment (DPIA) is meant to be an on-going project, rather than a single document or a mere product. In order to collect the full range of benefits that derives from the execution of a properly structured and implemented DPIA (namely, and amongst others, avoiding loss of trust and reputational damages, identifying and better managing risks, eluding avoidable costs and sanctions, and meeting or even exceeding legal compliance) you might want to structure your assessment in accordance with the following phases:

1. *Identify the need for a DPIA.*
2. *Describe the information flow*: identifying whether you handle personal information or not, information flows would need to be described: understanding where the data is held, to whom it is disclosed, who has access to it, how intelligible it is and where it may be transferred to is a necessary precondition to be satisfied in order to identify the potential risk your activities pose towards individuals' rights to privacy and data protection.
3. *Identify the risks*: using the questionnaire the risk scores.
4. *Identify how to address these risks*: Each vulnerability you discover and each potential violation of your data subjects' rights needs to be addressed with specific and targeted measures.
5. *Record the outcome assessment*: The record should contain an account of both the risks and the vulnerabilities you assessed and of the ways you plan to address them.
6. *Integrate the outcome of the assessment into your project or activities.*
7. *Consult with the relevant internal and external stakeholders:* The assessment aims at rendering your project more respectful of individuals' rights to privacy and data protection and to help you being compliant with the relevant legislation. The outcomes of the assessment, therefore, need to be turned into specific action points and integrated into your operations: the DPIA process does not stop with the production of a report, but continues with the implementation of its findings.

In order to identify how to better incorporate the findings of the assessment, and to evaluate the outcome of such integration, the relevant stakeholders, be they internal to your organization or external ones, would need to be recognized and consulted, possibly beforehand. Someone within your undertaking would accordingly need to be tasked with explaining how the outcome of the DPIA will be integrated within your activities (or – vice versa – why the findings of the assessment are not to be integrated) and with acquiring the relative feedback from the relevant stakeholders.

How should you create a DPIA Report?

A properly engineered and executed DPIA process should eventually produce a report, which is to take into consideration the entire lifecycle management of personal data, from the collection to their deletion. The report produced through the DPIA should be made available to the relevant stakeholders, provided that you undertake the appropriate measures to safeguard your undertaking and your data subjects from the disclosure of sensitive or confidential information. On request, the report should be made available to your national data protection authority as well. The report should contain, as a minimum, the following items:

1. A systematic description of the envisaged processing operations, the purposes of the processing and the legitimate interests pursued by the controller;
2. An assessment of the necessity and proportionality of the processing operations in relation to their purposes;
3. An assessment of the risks to the rights and freedoms of data subjects, including the risk of discrimination being embedded in or reinforced by the operation;
4. A description of the measures envisaged to address the risks and minimise the volume of personal data which is processed;
5. A list of safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the applicable data protection legislation;
6. A general indication of the time limits for erasure of the different categories of data;
7. An explanation which data protection by design and default practices have been implemented;
8. A list of the recipients or categories of recipients of the personal data;
9. Where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of appropriate safeguards;
10. An assessment of the context of the data processing.

DPIAs should not be considered in a vacuum: rather, they have a natural place within an organization’s general risk analysis and control practices. If you enact specific risk management methodologies, you might want to consider integrating your DPIA procedures within them: even if they do not focus explicitly on privacy and data protection, they provide for a framework within which those issues can be systematically addressed.

DPIAs, finally, are not meant to remain a static report, a one-off exercise: their execution should be reiterated regularly, two years after the previous assessment at the latest, and every time there is a significant modification of your activities, such as a new product, an organizational modification, a new partnership, and so on.

Cloud DPIA Questionnaire

ID	Question	Explanation	Question type	Response YES	Response NO	Action on YES	Action on NO	Score	Weight	Risk indicators
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.	**Y/N**	You have to comply with European Union laws.		Go to the next question	This Questionnaire is addressed to businesses and/or organisations which are established in the European Union. Since you are not established in the EU, this Questionnaire does not apply to you.	N/A – This answer is not counted in the overall score	0	N/A
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.	**Checkbox** - Web Browsing - Account and/or Subscription Management - Authentication and Authorization - Customization - Responding to User - (Service) Delivery - Software Downloads - Sales of Products or Services - Communications Services - Banking and Financial Management - Payment and Transaction Facilitation - Charitable Donations - Government Services - Healthcare Services - Education Services - Advertising, Marketing, and/or Promotion - News and Information- Arts and Entertainment - Surveys and Questionnaires - Online Gambling - Online Gaming - Search Engines - State and Session Management			Whichever option, go to the next question	Whichever option, go to the next question	(Number of ticked elements)/(total number of elements in the list)	1	SEN

ID	***Question***	***Explanation***	***Question type***	***Response YES***	***Response NO***	***Action on YES***	***Action on NO***	***Score***	***Weight***	***Risk indicators***
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.	**Checkbox** - Purposes related to the commercial objective of your undertaking *Health purposes:* - for preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services - for public interest in the area of public health, such as protecting against serious cross-border threats - for other reasons of public interest in areas such as social protection *Employment context:* - for purposes of the recruitment and job applications within the group of undertakings - for the performance of the contract of employment, including discharge of obligations, laid down by law and by collective agreements, - management, planning and organisation of work, health and safety at work, - for the purposes of the exercise and enjoyment of rights and benefits related to employment - for the purpose of the termination of the employment relationship - Purposes within the social security context - Processing for historical, scientific statistical or research purposes - enforcement of legal claims and/or compliance with law enforcement agencies -exercise of the right to freedom of expression or information (including in the media and the arts) - Other (Please specify)		Context specific responses. For instance: employment purposes: The processing of information of employees must be linked to the reason for which the information was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed.	Whichever option, go to the next question	Whichever option, go to the next question	If "health, employment, social security and law enforcement" then 1, else if "historical, scientific statistical or research purposes" then 1/4, else if "exercise of the right to freedom of expression or information" then 3/4, else 0.	1	SEN
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.'	Y/N			Go to Question 5	Go to Question 7	If 'Y' then 1/4 else 1.	1	DC C
5	How have you obtained the consent of individuals?	Consent requires prior information and an explicit indication of the intent to consent.	a) Consent is given directly by the individual by a statement (e.g. by a consent form) b) Consent is given directly by the individual by an affirmative action (e.g. by ticking a box) **c) Consent has been obtained implicitly by the individual (e.g. by merely use of the service or inactivity)**			Whichever option, go to the next question	Whichever option, go to the next question	If 'a' then 0, Else if 'b' then 1/4, Else if 'c' then 3/4	1	T

ID	***Question***	***Explanation***	***Question type***	***Response YES***	***Response NO***	***Action on YES***	***Action on NO***	***Score***	***Weight***	***Risk indicators***
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.	Y/**N**		Lack of ability to withdraw consent easily and without detriment may result in violation of data protection law	Go to the next question	Go to the next question	If 'N' then 6/8, else 0.	5	C DC
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?	Y/N			Go to the next question	Go to the next question	If 'Y' then 2/4 else 0	1	N/A
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.	**Checkbox** a) The individual has given his consent b) Processing is necessary for the performance of a contract between you and the individual whose information you process c) Processing is necessary for compliance with a legal obligation you have d) Processing is necessary in order to protect vital interests of the individuals whose information you process e) None of the above			Whichever option, go to the next question	Whichever option, go to the next question	N/A	N/A	N/A
9	Do you provide clear information about:		**Y/N Radio button** - the purposes for which you process personal information - the different types of information that you process - your identity		The individuals should have a clear overview of your identity, the types of information you process or the purposes for such processing, in order to exercise their rights. If you do not provide clear information you are not compliant with data protection regulations and your operations present risks for individuals.	Whichever option, go to the next question	Whichever option, go to the next question	For each checkbox not clicked add 1/3 to the score.	1	T C
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.	Y/N		The processing of non-relevant or over abundant may result in violation of data protection law	Go to the next question	Go to the next question	If 'N' then 7/8 else 0.	1	C
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?	Y/**N**		The individuals have to be given the ability to exercise their rights.	Go to the next question	Go to the next question	If 'N' then 6/8 else 0	5	DC C
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.	Y/N	The more rules you have to observe, the higher the likelihood that you breach one these.		Go to the next question	Go to the next question	If 'Y' then 6/8 else 0	1	C

ID	***Question***	***Explanation***	***Question type***	***Response YES***	***Response NO***	***Action on YES***	***Action on NO***	***Score***	***Weight***	***Risk indicators***
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.	Y/N	The mere collection of information is of different significance than the use of information in decision-making processes.		Go to the next question	Go to question 15	If 'Y' then 5/8 else 0	1	SEN
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?	Y/N	When the information you handle leads directly to decisions that can affect individuals, the impact of processing is likely to be greater than the one it would have if the processing activities did not have any direct consequence on the individual the information relates to		Go to the next question	Go to the next question	If 'Y' then 6/8 else 0	1	SEN
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.	Y/**N**		The individuals have the right to have their information corrected and updated. You have to ensure that you comply with this obligation.	Go to the next question	Go to the next question	If 'N' then 1 else 0	5	SEN
16	Does the information you process about the individual come from different sources?	Think, for instance, whether you obtain databases from other parties	Y/N	If you link information from different sources, the risk of processing incorrect and/or outdated information is higher and may impact your operations.		Go to the next question	Go to question 18	If 'Y' then 2/4 else 0	1	SEN
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.	Y/N		Transparency about your data processing practices may contribute to enhance trust of individuals to your organization/company	Go to the next question	Go to the next question	If 'N' then 1/4 else 0	5	T C
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.	Y/N	The purposes of your project should be clearly communicated to the individuals. This means that if you use existing personal information for new purposes you should obtain the consent of the individuals for the new purposes.		Go to the next question	Go to Question 23	If 'Y' then 4/8 else 0	1	SEN C
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.	Y/**N**		Personal information should not be processed for purposes which are not compatible with your original purposes.	Go to the next question	Go to the next question	If 'N' then 5/8 else 0	5	C

ID	***Question***	***Explanation***	***Question type***	***Response YES***	***Response NO***	***Action on YES***	***Action on NO***	***Score***	***Weight***	***Risk indicators***
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.	Y/N		Individuals should be clearly informed about the exact purposes of your processing operations. If you process information for additional purposes, different from your original ones, you should inform the individual for your new purposes of processing as well.	Go to the next question	Go to the next question	If 'N' then 1/4 else 0	1	C T
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.	Y/N			Go to the next question	Go to the next question	If 'N' then 2/4 else 0	1	C T
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.	Y/N			Go to the next question	Go to the next question	If 'N' then 2/4 else 0	1	C T
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.	Y/N	Certain types of information are more sensitive than others and should be safeguarded.		Go to the next question	Go to the next question	If 'Y' then 7/8 else 0	1	SEN
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	Y/**N**		Access to information is important to allow individuals to point out inaccuracies in the information you have about them	Go to the next question	Go to the next question	If 'N' then 7/8 else 0	5	T C DC
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)	Y/**N**		Incorrect information should be rectified or erased because you have an obligation to use correct and current information.	Go to the next question	Go to the next question	If 'N' then 1 else 0	5	C DC
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.	Y/N			Go to the next question	Go to the next question	If 'N' then 6/8 else 0	1	N/A
27	How often is the personal information you process updated?	Outdated information has a negative impact on the accuracy of information you process.	**Checkbox** - Frequently - When requested by the individual - Whenever necessary to comply with technological developments - Rarely - Never		Outdated information should be rectified or erased because you have an obligation to use current and correct information.	If frequently/when requested by the individual/whenever necessary to comply with technological developments go to question 29	If *Rarely or Never,* go to the next question	If 'a then 0, Else if 'b' then 0.2, Else if 'c' then 0.5, Else if 'd' then 0.8, Else 1	1	N/A

ID	Question	Explanation	Question type	Response YES	Response NO	Action on YES	Action on NO	Score	Weight	Risk indicators
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.	- High - Medium - Low - None			Whichever option, go to the next question	Whichever option, go to the next question	If 'High' then 1 Else if 'Medium' then 2/3, Else if Low then 1/3, Else 0	1	N/A
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.	Y/N/**IDK**			Whichever option, go to the next question	Whichever option, go to the next question	N/A	N/A	N/A
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	Y/**N**	Having a Data Security Policy allows you to check your compliance to Data Protection Regulations	The absence of Data Security Policy is able to put at risk the protection of personal information and the rights of individuals.	Go to the next question	Go to the next question	If 'N' then 5/8 Else 0	5	SEC
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.	Y/N	The application of technical and organizational security measures from the outset of your activities allows you to take into consideration potential risks for the protection of privacy of individuals.	Lack of the application of technical and organizational security measures from the outset of your activities may put the rights of individuals at stake.	Go to the next question	Go to the next question	If 'N' then 4/8 Else 0	1	SEC
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.	Y/N		Processing of information of sensitive nature, such as to race or ethnic origin, political or sexual orientation, religion or gender identity, deserves specific protection.	Go to the next question	Go to the next question	If 'N' then 4/8 Else 0	1	SEC
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.	Y/N		Trained employees are able to ensure the compliance of your operations to the relevant data protection regulations.	Go to the next question	Go to the next question	If 'N' then 4/8 Else 0	1	SEC
34	How often are your Security and Privacy Policies updated?		Radio button - Frequently - Whenever necessary to comply with technological developments - Rarely - Never			Whichever option, go to the next question	Whichever option, go to the next question	If 'a' then 0 Else if 'b' then 1/3, Else if 'c' then 2/3, Else 1	1	SEC

ID	Question	Explanation	Question type	Response YES	Response NO	Action on YES	Action on NO	Score	Weight	Risk indicators
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.	[**Checklist**] - Personal information is kept confidential - Access control is enforced - Segregation of duty is used - Special authorization for personnel who access the information - Compliance with further regulations is ensured - Use of personal information are properly documented - Procedures to maintain personal information use up-to-date regularly - Subcontractors follow the same guidelines on documenting the use of information - Procedures to notify individuals, when necessary, are in place - Procedures to take into account the impact of the information lifecycle - Procedures to record individuals' requests for correction of information - Specific procedures to respond to Law Enforcement access or court orders - Modalities to express, withhold, or withdraw informed consent to the processing - **Anonymization** - **Pseudonymisation** - **Encryption** - Aggregation - Separation - Limitation of usage - Data segregation - Sticky Policies - All of the above - None of the above			Whichever option, go to the next question	Whichever option, go to the next question	1-(Number of ticked elements)/(total number of elements in the list). If 'None of the above' then 1	1	SEC DC
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.	Y/N	If you encrypt your information before putting it on to the cloud, you are the only party that has access to personal information. All other parties who are exposed to the information in an already encrypted form cannot have access to personal information.		Go to the next question	Go to the next question	If 'Y' then 0, Else 1	5	SEC DC
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	Y/N/IDK		The absence of specific measures in order for the protection of personal information to be ensured in the event of physical or technical incident sets at stake the rights of individuals and especially the protection of their personal information.	Go to the next question	N/IDK -> Go to the next question	If 'N' then 2/8, Else 0	1	SEC

ID	Question	Explanation	Question type	Response YES	Response NO	Action on YES	Action on NO	Score	Weight	Risk indicators
38	Do you take action in order to notify individuals in case of (security) incidents?	E.g. by sending emails.	Y/N			Go to the next question	Go to the next question	If 'N' then 5/8, Else 0	1	SEC C T
39	What do you do to minimize the damages of physical, technical and/or security incidents?		Checklist - Segregation of data bases - Limitation of use/transfer functionalities on system layer - Separation on system layer - Multi-tenancy limitations - Physical separation of infrastructure - None of the above - Others (please indicate)		None of the above > Enacting specific procedures reduces the impact of any unwarranted incident that may happen.	Whichever option, go to the next question	Whichever option, go to the next question	1-(Number of ticked elements)/(total number of elements in the list). If 'None of the above' then 1	1	SEC
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.	Y/N			Go to the next question	Go to the next question	If 'N' then 1/4, Else 0	1	DC
41	For how long do you store the information you are dealing with?		[checklist] - Only for the completion of the project's purposes - Information is retained for a certain time after the project has been completed - Information is retained for the possibility of future uses or new purposes - Until individual requests for erasure			Whichever option, go to the next question	Whichever option, go to the next question	If 'a' then 0, Else if 'b' then 1/3, Else if 'c' then 2/3, Else 1	3	N/A
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?	Y/N		All parties involved should be aware of any transferring in order for an adequate level of protection of the information processed to be ensured.	Go to the next question	Go to question 44	If 'Y' then ¾, Else 0	1	DS DC
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.	Y/N/IDK			Go to the next question	N/IDK -> Go to the next question	If 'N' then 7/8, Else 0	1	DS DC C
44	Do you sell, rent or by any means disseminate information to third parties?		Y/N	By selling or renting the information you process to third parties you may put at risk the rights of individuals.		Go to the next question	Go to the next question	If 'Y' then 4/8, Else 0	1	DS
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.	Y/N			Go to the next question	If not on list go to 47	If 'Y' then and 'N' for Question 45 then 6/8, Else 0	1	TB

ID	Question	Explanation	Question type	Response YES	Response NO	Action on YES	Action on NO	Score	Weight	Risk indicators
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	[checklist] - Andorra - Argentina - Australia - Canada - Switzerland - Faeroe Islands - Guernsey - Israel - Isle of Man - Jersey - New Zealand - Uruguay - U.S.			Go to the next question	If not on the list -> Go to the next question	N/A (already included in the previous question)	0	TB C
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.	Y/N/IDK			Go to the next question	N/IDK -> Go to the next question	If 'N' then or 'IDK' then 6/8 else 0	1	SEC TB C
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.	a) owned by or operated for only me (private cloud) b) is owned by or operated for a specific group of users with common interests in a shared manner (community cloud) c) is shared amongst multiple users (public cloud)			Whichever option, go to the next question	Whichever option, go to the next question	If 'a' then 0, Else if 'b' then ½ Else if 'c' then 1	1	C
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.	Y/N			Go to the next question	Go to the next question	If 'Y' then 1, Else 0	If 'Y' then 1 Else 0	N/A
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).	Y/N/IDK		The proposed General Data Protection Regulation explicitly recognizes the right of individuals to transfer their information to other platforms (data portability).	Go to the next question	N/IDK -> Go to the next question	If 'N' or 'IDK' then 1, Else 0	5	DC

Further information

- Rehab Alnemr, Erdal Cayirci, Lorenzo Dalla Corte, Alexander Garage, Ronald Leenes, Rodney Mhungu, Siani Pearson, Chris Reed, Anderson Santana de Oliveira, Dimitra Stefanatou, Katerina Tetrimida, Asma Vranaki. “A Data Protection Impact Assessment Methodology for Cloud”, in the Proceedings of the Annual Privacy Forum, Springer LNCS, 2015.
- Rehab Alnemr. Data Protection Impact Assessment: A technologist’s perspective. A Technologist's Perspective. March 2016, Privacy Laws and Business Magazine, UK.

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).