
D:C-6.2 Prototype for the data protection impact assessment tool

Deliverable Number	D36.2
Work Package	WP 36
Version	Final
Deliverable Lead Organisation	SAP
Dissemination Level	PU
Contractual Date of Delivery (release)	30/09/2014
Date of Delivery	20/10/2014

Editor

Anderson Santana de Oliveira (SAP)

Contributors

Alexander Garaga, Anderson Santana de Oliveira (SAP), Erdal Cayirci (UiS), Lorenzo Dalla Corte, Ronald Leenes, Rodney Mhungu, Dimitra Stefanatou, Katerina Tetrimida (TiU), Rehab Alnemr, Massimo Felici, Siani Pearson (HP), Asma Vranaki (QMUL)

Reviewers

Jesus Luna, Konstantinos Mantzoukas (CSA), Thomas Rübsamen (HFU)

Executive Summary

The work package C6 – Risk and Trust Models has the ambitious goals to devise risk and trust models for cloud computing supporting accountability mechanisms and practices. As the scope of A4Cloud is centred on personal data protection in the cloud, we target in this work Data Protection Impact Assessments (DPIAs) and risk assessments for the cloud.

This deliverable presents a cloud adoption risk assessment model for evaluating cloud service, ideally before the service is contracted, risks using data aggregated from real cloud services. It is a continuation of the work reported in D36.1 (de Oliveira et al, 2014), which introduces a trust model allowing for cloud consumers to rely on trusted third parties in order to customize which elements of transparency they need to know and how to monitor them. We combine this approach with a renewed methodology for data protection impact assessments, building on existing knowledge on the topic, but taking an “individual-centric approach”, meaning that the method helps users to understand the risks to the rights of data subjects, as the data protection impact is assessed.

The DPIA method is based on successive questionnaires, for the initial screening, and for the full screening for a given project. They were tailored to satisfy the needs of Small and Medium Enterprises (SMEs) that intend to process personal data in the cloud. The approach takes into consideration the principles put forward in the proposed General Data Protection Regulation, whose new requirements for DPIAs were analysed. These features are implemented by the Data Protection Impact Assessment Tool prototype also described in this deliverable.

Finally, the risk and data protection impact assessment methodologies are applied to a use case. We analyse the A4Cloud Business Use Case 2, defined in the B-3 use case development work package, where an SME extends its ERP functionality with a SaaS to improve its relationship with its customers. Such exercise provided insights and allowed to realize improvements in the methodology, questionnaire, and tool.

Table of Contents

Executive Summary.....	2
1 Introduction.....	5
1.1 Related Work	5
1.2 Structure of the document.....	7
2 DPIA's in the EU Data Protection Reform.....	8
2.1 The DPD on DPIAs	9
2.2 The European Data Protection Reform – The Commission on DPIAs	11
2.3 The Parliament on the proposed GDPR	12
2.4 The Council on the proposed GDPR	16
2.5 Conclusion	18
3 DPIA questionnaires.....	21
3.1 Methodology.....	21
3.2 Structure.....	24
3.3 Discussion	27
4 Cloud Adoption Risk Assessment Model	30
4.1 Risk Level Computation	30
4.2 Control Implementation Data Collection	32
4.3 The Vulnerability Parameter for a CSP	33
4.4 Relative Risk Assessment with Posterior Articulation of CSC Preferences	34
4.5 Limitations and Future Work	34
5 Data Protection Impact Assessment Tool	36
5.1 Tool Interface and Data Flow	36
5.2 Tool Components and Architecture	38
5.3 Tool Implementation.....	39
6 Use case analysis	41
6.1 Cloud adoption risk assessment.....	41
6.2 Data protection impact assessment.....	45
7 Conclusions.....	47
8 References	48
9 Appendices.....	50
9.1 Cloud security risk assessment input.....	50
9.2 Cloud DPIA Questionnaire	63
9.3 DPIA Screening for Business Use Case 2.....	84

Index of figures

Figure 1 CARAM process and data flow	30
Figure 2 ENISA definition of risk levels	31
Figure 3 DPIAT initial screen.....	37
Figure 4 DPIAT tooltip displaying information about the selected options	37
Figure 5 DPIAT Components	38
Figure 6 Technologies used in the DPIAT implementation	40
Figure 7 Conceptual overview of the cloud-based ERP business use case	41
Figure 8 Cloud Risk Assessment Plugin Screenshot.....	44

Index of tables

Table 1 CAIQ example answers.....	32
Table 2 The control groups in CAIQ	33
Table 3 The categorization of the answers given to the questions in the CAIQ	33
Table 4 Relevant assets for the Use Case.....	43
Table 5 Weight factor for the risk scenario categories	44
Table 6 ENISA's list of risk scenarios and their categories	50
Table 7 ENISA's list of vulnerabilities	50
Table 8 ENISA's list of assets	51
Table 9 Mapping CAIQ questions to vulnerabilities	52
Table 10 Mapping ENISA risk scenarios to A4CLOUD risk categories	55
Table 11 Vulnerability Parameter for BUC 2 SaaS	55
Table 12 Vulnerability Indices for the BUC2 SaaS.....	57
Table 13 CAIQ answers for the MarcheAzur SaaS.....	58

List of Acronyms

D

Data Protection Directive (DPD) · 9
Department of Homeland Security (DHS) · 7

G

General Data Protection Regulation ('GDPR') · 9
Governance, Risk, and Compliance (GRC) · 6

H

HP Privacy Advisor (HP PA) · 7

I

Information Commissioner's Office (ICO) · 6

O

Organisation for Economic Cooperation and
Development (OECD) · 10

P

Privacy and Electronic Communications Regulations
(PECR) · 7
Privacy Impact Assessments (PIAs) · 6

1 Introduction

Privacy Impact Assessments (PIAs) allow to identify the risks of a project to the rights of data subjects concerning their personal data. It is a systematic process to elicit threats to the privacy of individuals, to identify the procedures and practices in place to mitigate these threats, and to document how the risks were addressed in order to minimise harm to data subjects (ICO 2009, CNIL 2012). PIAs have been recognised as a key topic for data protection governance in Europe, as it will become mandatory according to the ongoing data protection legal framework reform¹.

Accountable organisations will embrace PIAs as part of their overall risk management practices, as advocated in (Trilateral Research & Consulting, 2013). Unfortunately today there is a lack of tool support for organisations to perform PIAs of cloud services. In this deliverable we present the design of the A4Cloud Privacy Impact Assessment tool. The tool considers a number of information sources from which cloud specific risks and existing countermeasures can be collected and evaluated, in the process of supporting privacy impact assessments for the cloud. We also propose an updated PIA questionnaire with respect to existing standards and recommendations, building on the expertise of our partners on legal research and also on the security risk assessment expertise of the further partners. One of the goals is to provide guidance in the process of first determining the need of a full-fledged PIA, and then, of conducting the assessment in a friendly yet didactic manner, as the user performing the assessment provides information about the project under evaluation and its organisational practices, combined with the selection of a cloud service provider.

1.1 Related Work

Privacy impact assessments are already being rolled out as part of a process to encourage privacy by design (Trilateral Research & Consulting, 2013): in November 2007 the UK Information Commissioner's Office (ICO) (an organisation responsible for regulating and enforcing access to and use of personal information), launched a Privacy Impact Assessment (PIA) process (incorporating privacy by design) 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. Similar methodologies exist and can have legal status in Australia, Canada and the US (Tancock et al., 2010). The methodology aims to combat the slow take-up to design in privacy protections from first principles at the enterprise level. Usage is increasingly being encouraged and even mandated in certain circumstances by regulators, as considered further in the following section.

There has been a great deal of related work, in terms of the specification of privacy requirements and the translation of these into machine-readable policies (see for example WP C-4 for further analysis). There are also Governance, Risk, and Compliance (GRC) tools that are related, such as RSA Archer Compliance Management system²

The role of a risk-based approach in data protection has been considered by a number of parties, including: as an assessment of the relative values of such an approach (Bennett and Raab, 2006); modifying the original OECD data protection principles to take this into account (OECD, 2013); analysing the relationship with accountability (Theoharidou et al, 2013; Felici & Pearson, 2014) and recent regulatory analysis (Article 29 WP, 2014; CIPL, 2014).

In terms of automation within the privacy impact assessment process, there are a few systems that have attempted this in various contexts which we shall consider further below.

In Canada the Treasury Board Secretariat provides an e-learning tool for government employees interested in learning more about privacy and PIAs and how to complete them. The e-learning tool consists of two courses (e.g. Overview, and Manage/Monitor), and a PIA Assistant to help users complete PIAs (Treasury Board Secretariat Canada, 2003). Furthermore, a new self-assessment tool,

¹ http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_dp_plenary_vote_140312_en.pdf

² <http://uk.emc.com/security/rsa-archer/rsa-archer-compliance-management.htm>

aimed at private-sector organisations, particularly small and medium-sized businesses, was recently launched in Canada (e.g. May 2011). The tool developed jointly by the federal, Alberta and British Columbia privacy commissioners' offices is called "*Securing Personal Information: A Self-Assessment Tool for Organizations*", where it is hoped that the tool may help businesses better safeguard the personal information of customers and employees, and may help prevent breaches of personally identifiable information (PII) (Office of the Privacy Commissioner of Canada, 2011). The tool is a detailed online questionnaire that helps organisations gauge how well they are protecting personal information and meeting compliance standards under Canada's private-sector privacy law on both federal and provincial levels. The questionnaire is complex and not easy to navigate, as it involves dozens of "yes", or "no" questions divided up into seventeen different categories including: network security, access control, incident management, and database security. However it offers some flexibility by allowing users to focus on areas most relevant to their own enterprise.

The US Department of Homeland Security (DHS) employs a PIA tool called the Privacy Threshold Analysis that helps users determine whether a PIA is required under the E-Government Act of 2002 and the Homeland Security Act 2002 (United States Department of Homeland Security, 2007). In the UK, the PIA Guidelines provide a number of screening questions to help users decide whether a Full-Scale PIA or a Small-Scale PIA is warranted. The Guidelines also include a number of questions for a privacy law compliance check, and a Data Protection Act (1998) compliance check. Templates are also included within the Guidelines for Data Protection compliance and the Privacy and Electronic Communications Regulations (PECR) (Information Commissioners Office, 2009).

The evaluation processes involved in these PIA tools consist of simple questionnaires, whereby most of the questions require a "Yes" or "No" response. Analysis of the PIA tools suggests that they are mainly based upon a simple "decision-tree" approach. This approach is commonly used for simple reasoning, as it is both a knowledge representation scheme and a method of reasoning about that knowledge. In addition, the PIA tools produced by the different jurisdictions are mainly procedure-based (e.g. whereby a number of specified steps are used to reach desired outcomes), and their granularity are coarse-grained (e.g. consist of fewer larger components). Finally, the PIA tools are Web applications where both data and the applications are at the server-side, and do not take into account the cloud or any of its characteristics.

The following are PIA automated systems that are worthy of particular mention:

- A prototype decision support tool developed by the PRAIS project (Harbird et al, 2010). This tool enables personnel working with personal information to assess the privacy implications of information sharing actions dynamically and to share information with confidence, whether verbally, or electronically. This has been achieved by accommodating the daily routines of social care staff from the outset, with the tool managing users' consent and the needs and requests of information from the participants.
- HP Privacy Advisor (HP PA). This is an intelligent online rule-driven system that assesses activities that handle personal data within HP and provides privacy by design guidance (Pearson & Sander, 2012). It is a web-based decision support system used internally within HP to assess risk and degree of compliance for projects that handle personal data and to guide individual employees in their decisions on how to handle different types of data. HP PA elicits privacy-relevant information about a project via a customised sequence of questions (Pearson, 2010). It uses a dynamic interface to minimise unnecessary questions and maintains a record of activities, capturing global privacy knowledge that is too complex to be easily captured via decision trees, while avoiding unpredictable system behaviour and ensuring completeness (Pearson et al., 2009).
- A privacy impact assessment tool prototype based upon ICO guidelines related to UK Data protection Act, allowing appropriate stakeholder views and input and using confidences within the knowledge representation to allow assessment of the value of the input as well as customisation of risk indicator values (Tancock et al, 2010).

Use of DSSs for cloud computing and PIAs is a very new field and there are few systems available, although there is some work targeted at the areas of clinical decision applications³, and life science enterprise solutions (CambridgeSoft, 2010). Prior work includes tools for cloud assessment, notably vendor security assessment tools⁴, the Microsoft “Security Assessment Tool” designed to help find weaknesses in an IT security environment⁵, cloud security guidance (for example, from Enisa (Enisa, 2009), NIST (NIST, 2011), ICO (ICO, 2012) and CNIL (CNIL, 2012)), CSA GRC stack (CSA, 2013), privacy impact assessment of cloud environments (Tancock et al, 2012) and decision support tools for cloud service provisioning (Sander & Pearson, 2010). The latter is based on the same underlying approach as HP PA.

The work we conducted in A4Cloud builds on the body of knowledge and recommended practices mentioned above, adjusting the DPIA process and questionnaire to make it informative, user-centric and synthetic. It differs from the previous works by focusing on a profile of SMEs wishing to move to the cloud. Additionally, our approach for assessing cloud risks is founded on actual information generated voluntarily by CSPs, and collected from the CSA Security, Trust & Assurance Registry (STAR)⁶.

1.2 Structure of the document

The remaining sections of the deliverable are organized as follows:

- Section 2 presents an overview of the new obligations concerning DPIAs under the proposed European Regulation for Data Protection
- Section 3 introduces the A4Cloud approach for DPIA, with a revised questionnaire bringing in data protection concerns in a understandable manner to lay users
- Section 4 presents our approach for assessing cloud risks which takes into account concerns for the cloud service consumers while dealing with hard trust elements obtained from the service providers
- Section 5 presents the design and implementation of the DPIA tool
- Section 6 presents the evaluation of the business use case 2 in terms of cloud and data protection risks using the methodologies presented here
- Section 7 concludes the deliverable

³ <http://www.eweek.com/c/a/Health-Care-IT/IBM-Aetna-Join-for-New-CloudBased-Health-Care-Support-System-667092>

⁴ <https://sharedassessments.org/>, http://www.privacyguidance.com/eMy_Mgmt_Tools.html

⁵ <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=12273>

⁶ <https://cloudsecurityalliance.org/star/>

2 DPIA's in the EU Data Protection Reform

In view of designing a DPIA tool, it is necessary to examine how DPIAs are regulated in the context of European Data Protection Law.

The current European data protection framework is under revision. The Data Protection Directive (DPD) seems to be inadequate to respond to the new and constant challenges of globalisation and of the increasingly rapid technological developments⁷. In this context, in 2012, the European Commission proposed a comprehensive reform of the European privacy and data protection milieu in order for “a more comprehensive and coherent policy on the fundamental right to personal data protection⁸” to be adopted. This revision of the European Union’s data protection framework will be enacted (also) through the upcoming General Data Protection Regulation (GDPR)⁹. The legal instrument of the Regulation, with its direct applicability by all member states, seems indeed to be the most appropriate solution in order to guarantee a uniform level of protection of personal data to be ensured throughout the European Union. The proposed GDPR aspires to contribute to the reduction of legal fragmentation and the enhancement of legal certainty in the field of the protection of personal data by creating common rules for data protection.

In this context, the general obligation to notify the supervisory authorities about the processing of personal data, which is stipulated in Article 18 of the DPD, was considered insufficient in order for an effective protection of personal data to be ensured¹⁰, leading to the foreseen adoption of more effective procedures and mechanisms, such as Data Protection Impact Assessments¹¹ (DPIAs)¹². However, it should be noted that while the current DPD does not provide explicitly for the mandatory performance of DPIAs on an European level, “(t)he term PIA has certainly been known in some European countries, however, not least The Netherlands¹³”, and in several non-European ones¹⁴ as well.

The European regulator took into account the existing gap by providing explicitly for DPIAs in the GDPR to be executed under specific circumstances. In particular, the Parliament introduced (in Articles 32a and 33 in the European Parliament’s first reading version) the concept of a risk-based data protection management life cycle, an important part of which is the notion of DPIA¹⁵. The approach of the European Parliament seems to incorporate the concept of risk into the DPIA mechanism as a helpful tool in decision making process due to its flexibility, as it can be adjusted and adapted depending on the

⁷COM(2012) 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.

⁸Ibid, p. 2.

⁹Ibid.

¹⁰COM(2012) 11 final 2012/0011 (COD), Recital 70 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.

¹¹Or Privacy Impact Assessments (PIA). Given the lack of a stringent distinction between the concept of PIA and the one of DPIA, on one hand, and the lack of a common definition of neither of the two, the terms will be used as synonyms, favouring the use of 'PIA' when referring to the period before the GDPR proposal by the Commission.

¹²COM(2012) 11 final 2012/0011 (COD), Recital 70 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.

¹³Clarke, Roger, “Privacy impact assessment: Its origins and development”, *Computer law & security review* 25.2 (2009): p. 129.

¹⁴e.g. Canada, Australia, New Zealand, Hong Kong.

¹⁵“In essence, PIA is a process to diagnose risks and propose safeguards [...] a procedural mechanism of privacy protection”, and “risk assessment is a protecting procedure that is related to a liability regime based on harm and culpability”: Costa, Luiz, “Privacy and the precautionary principle”, *Computer Law & Security Review* 28.1, 2012: 20-21. See also Wright, David, “The state of the art in privacy impact assessment”, *Computer Law & Security Review* 28.1, 2012: 55, where PIAs are defined as “a methodology for identifying risks to privacy posed by any new project [...] and devising solutions to avoid or mitigate those risks”. The same article (p. 57) frames further PIAs in the scope of risk management: “(m)ost PIA guidance documents say that PIA should be viewed as part of an organisation’s risk management practice. [...] PIAs are about identifying risks and finding solutions. They should not be seen as somehow distinct from risk management, as simply a compliance check. A PIA is more than a check that a project complies with existing legislation or privacy principles”. Again, “PIAs have been thus defined as a systematic risk assessment tool that can be usefully integrated into decision-making processes”: Warren, Adam, et al. “Privacy Impact Assessments: International experience as a basis for UK Guidance”, *Computer Law & Security Review* 24.3, 2008: 234.

particularities and specificities of each project to be assessed¹⁶. Indeed, the significance of risk-based approaches has been pointed out by different organisations, such as, for instance, the Organisation for Economic Cooperation and Development (OECD) which states that “risk-based approaches to the design of regulation and compliance strategies can improve the welfare of citizens by providing better protection from hazards, more efficient [government] services and reduced costs for business¹⁷”, and the concept of risk – which could be defined as the likelihood of a negative event happening – is arguably closely intertwined with the one of impact¹⁸.

The analysis of this section will try to clarify the approaches towards the adoption of DPIAs by three Institutions of the European Union, namely the European Commission (Commission), the European Parliament (Parliament) and the European Council (Council). In this context, the analysis will start with a section on how the current DPD deals with DPIAs, which will then be followed by a part on how the different versions of the GDPR deal with DPIA. The discussion aims to bring about the legal requirements surrounding the performance of DPIAs under European Data Protection Law, that need to be taken further into account when developing a DPIA tool. This analysis anchors the examination expounded in section 4 on how DPIAs should react and adapt to a cloud computing environment.

2.1 The DPD on DPIAs

The DPD does not provide explicitly for the mandatory adoption and performance of DPIAs as necessary assessments to be performed by controllers and/or processors in order to protect and manage the personal data of their data subjects. However, in Article 20 of the DPD it is foreseen that “*processing operations likely to present specific risks to the rights and freedoms of data subjects*” shall be subject to prior check¹⁹ by the national DPAs, before the start of any processing operations²⁰. In this respect, Article 20 of the DPD seems to implicitly consider the notion of PIA in spite of the absence of a direct and explicit reference to it: prior checking as a precursor to PIAs and DPIAs.

This prior checking requirement stipulated in Article 20 of the DPD has been transposed into the national legislation of the majority of Member States²¹. However, there is still a heterogeneous approach amongst them in relation to the enucleation of which categories of processing operations are likely to present specific risks²². Most of the national DPAs, at least in practice, follow specific procedures and implement an additional set of tools in order to assess the processing operations which are likely to present specific risks²³ – as PIAs and DPIAs are²⁴.

¹⁶De Hert, P., Kloza D., Wright D., “*Recommendations for a Privacy Impact Assessment Framework for the European Union*”, Deliverable D3, PIAF, 2012, p.10.

¹⁷Organisation for Economic Cooperation and Development, “*Risk and Regulatory Policy*”, n.d, available at <<http://www.oecd.org/gov/regulatory-policy/riskandregulatorypolicy.htm>>, last accessed on 01 July 2014.

¹⁸See Costa, Luiz, “*Privacy and the precautionary principle*”, *Computer Law & Security Review* 28.1, 2012: p. 18 ss.

¹⁹Albeit the idea of a compliance prior check is not new in European pre-DPD laws: “*Data protection laws that predated the OECD Guidelines (e.g. those of Hesse 1970, Sweden 1973 and Austria, Denmark, France and Norway all of which passed laws in 1978) commonly required registration or licensing, and a check was necessary to ensure that the data controller’s behaviour was in compliance with the law. Flaherty (1989, p. 405) documents instances where pre-decisional assessments were occasionally used in some European countries such as the Scandinavian countries and the U.K., and Bygrave (2002) points out that the Norwegian Data Inspectorate was required to assess “whether the establishment and use of the register in question may cause problems for the individual person” (s. 10, Norwegian Personal Data Registers Act of 1978, since superseded)*”: Clarke, Roger, *Ibid.*: p. 125.

²⁰“*PIA walks at a different pace in Europe. The European legislation does not establish an obligation to carry on PIAs. Instead, Article 20 of Directive 95/46/EC imposes the obligation of conducting previous control of operations that can pose risks to privacy and data protection*”: Costa, Luiz, *Ibid.*: 18.

²¹According to a questionnaire addressed to 30 National Data Protection Authorities (DPAs), which include the 27 National DPAs of the European Union along with the DPAs of Lichtenstein, Norway and Macedonia, the National DPAs were asked to answer the question (among others) on whether the prior checking requirement stipulated in Article 20 of the DPD is provided for in their national legislation. See: Le Grand G. and Barrau E. ‘*Prior Checking, a Forerunner to Privacy Impact Assessments*’ in David Wright, Paul De Hert (eds), “*Privacy Impact Assessment*”, Law, Governance and Technology Series, Volume 6, Springer, pp. 97-116.

²²Le Grand G. and Barrau E. ‘*Prior Checking, a Forerunner to Privacy Impact Assessments*’ in David Wright, Paul De Hert (eds), *Ibid.*, pp. 97-116..

²³Le Grand G. and Barrau E. ‘*Prior Checking, a Forerunner to Privacy Impact Assessments*’ in David Wright, Paul De Hert (eds), *Ibid.*, pp. 97-116.

²⁴Le Grand G. and Barrau E. ‘*Prior Checking, a Forerunner to Privacy Impact Assessments*’ in David Wright, Paul De Hert (eds), *Ibid.*, pp. 97-116.

Moreover, PIAs and DPIAs seem to have been generally adopted as a necessary organisational measure for minimizing privacy risks, albeit in a particular form, and as a part of a separate concept: the embedding of privacy and data protection features into the design specifications of information technologies from the very outset of any project or operation²⁵ – the concept of *Privacy by Design*²⁶, which is seemingly enshrined in article 17 of the DPD – arguably presupposes an assessment to be done as a necessary antecedent.

In particular, Article 17 refers directly to the appropriate technical and organisational measures in order for the security of processing of personal data to be ensured: “*Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected*”²⁷. Such technical and organizational measures are also specified in Recital 46, which emphasizes the importance of the adoption of “*appropriate [technical and organizational] measures, both at the time of the design of the processing system and at the time of the processing itself, in order to ensure [...] an appropriate level of security [by] taking into account [...] the risks inherent in the processing and the nature of the data*”²⁸. In this respect, the significance of these mechanisms lies in the fact that considerations related to a project's impact on data subjects' privacy and data protection can be integrated in its early stages, in order to minimize any potential security risks²⁹ from its very outset. From this perspective, the provision of Article 17 of the DPD seems to affirm the view of the Information Commissioner's Office (ICO) that Impact Assessments on Privacy and Data Protection constitute an integral part for the completion of Privacy by Design requirements³⁰.

However, under the impact of globalization and rapid technological advancement, the general provision for Privacy by Design mechanisms, along with the broad and flexible approach of the prior checking requirement stipulated in article 20, do not seem to suffice in order for an adequate level of protection of personal data to be ensured across the European Union. This looks evident, when considering the fact that Member States have adopted a fragmented approach with regard to prior checking, which has redound to function, in most cases, as a formal procedural step³¹.

Notwithstanding the fact that, at least under the DPD, PIAs are not mandatory, the European institutions explicitly recognized their importance – the Commission, for instance, made no mystery³² of its intention to make PIAs mandatory. The following paragraphs will deal with the increased importance that the notion of PIA (or DPIA, seemingly depending on the wording preferred) grew to have in the upcoming European data protection reform package, taking into consideration first the Commission's version, and then the amendments suggested by the Parliament, on one hand, and by the Council on the other.

²⁵Cavoukian A., “*Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*”, Information and Privacy Commissioner, Ontario, Canada, August 2011, pp. 14-15.

²⁶The Privacy-by-Design concept has been developed by Ann Cavoukian, Information & Privacy Commissioner in Ontario, Canada in order to “*address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems*”. See: Cavoukian A., “*Privacy-by-Design: The 7 Foundational Principles*”, Information and Privacy Commissioner, Ontario, Canada available at <<http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf>>.

²⁷Article 17 of the 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, O.J. L 281, 23/11/1995 P. 0031 – 0050.

²⁸Recital 46 of the 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, O.J. L 281, 23/11/1995 P. 0031 – 0050.

²⁹Information Commissioner's Office, “*Benefits of taking a Privacy-by-Design Approach*” available at <http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design> accessed on 15 July 2014.

³⁰Information Commissioner's Office, “*Conducting privacy impact assessments code of practice*”, ICO, 2014.

³¹Le Grand G. and Barrau E. ‘*Prior Checking, a Forerunner to Privacy Impact Assessments*’ in David Wright, Paul De Hert (eds), *Ibid.*, pp. 97-116.

³²See Wright, David, “*The state of the art in privacy impact assessment*”, Computer Law & Security Review 28.1, 2012: 54, and European Commission, COM(2010) 609 final, Brussels, 4 nov. 2011.

2.2 The European Data Protection Reform – The Commission on DPIAs

As mentioned, a reform³³ of the current European data protection legislation was proposed by the European Commission in 2012 in order for a *more comprehensive and coherent policy on the fundamental right to personal data protection*³⁴ to be adopted. The proposed reform of the DPD has taken the form of a Regulation, which seems to be the most appropriate solution in order for a uniform level of protection of personal data to be ensured throughout the European Union: a Regulation is directly applicable as such, without having to be transformed into national law as Directives require, which means that all Member States should relish the same level of protection of personal data³⁵. In this respect, the proposed GDPR aspires to contribute to the reduction of legal fragmentation and the enhancement of legal certainty in the field of the protection of personal data by creating common rules for data protection. This paragraph delves into PIAs as framed by the Commission's GDPR proposal. The proposed GDPR recognizes in Recital 7 that the current DPD has not managed to ensure a solid data protection framework implementation across the EU. The different approaches adopted by Member States with regard to the level of protection of the rights and freedoms of individuals have redounded to the emergence of *legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals associated notably with online activity*³⁶. In this respect, it seems that it aims at taking into consideration the new and constant challenges and risks for the protection of personal data which arise due to the rapid technological development and the continuous personal data flows, particularly via the online environment.

Moreover, Article 33 of the proposed GDPR (in the European Commission's version) introduces the obligation of data controllers and/or processors to carry out a Data Protection Impact Assessment (DPIA) prior to the start of their risky processing operations. In particular, Article 33(1) in the European Commission's text foresees that, if the controller or the processor performs processing operations which present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, they (the controller, or where applicable the processor) shall carry out an assessment of the impact of their processing operations on the protection of personal data.

In addition to this, the second paragraph of Article 33 (in the European Commission's proposal for a GDPR) stipulates an indicative list of these processing operations which present specific risks. This list includes, *inter alia*, processing operations which refer to "a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual" (Article 33(2)(a) in the European Commission's version), *information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale*" (Article 33(2)(b) in the European Commission's version) and "monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale" (Article 33(2)(c) in the European Commission's version). The adoption of an indicative list – instead of a more exhaustive one, as proposed by the Council³⁷ – can arguably help in stimulating considerations of possible impacts on privacy and data protection in the initiation of processing operations³⁸.

³³COM(2012) 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.

³⁴COM(2012) 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. 2.

³⁵COM(2012) 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. 6.

³⁶COM(2012) 11 final 2012/0011 (COD) Recital 7, 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.

³⁷See below.

³⁸Wright D., Finn R., Rodrigues R., "A Comparative Analysis of Privacy Impact Assessment in Six Countries", *Journal of Contemporary European Research*, 2013, 9 (1), pp. 160-180.

Despite the fact that the proposed GDPR does not include a definition on DPIA, Article 33(3) (in the European Commission's version) indicates the minimum requirements which a DPIA shall contain. In particular, a DPIA *"shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned"*. It is apparent that, as in the case of the non-exhaustive list of processing operations, here, the European Commission provides just for the minimum necessary specifications as well.

In this context, the minimum requirement approach seems to affirm the concept that a DPIA shall not be considered as a mere compliance check tool³⁹, but as a more nuanced and comprehensive assessment process. To support this argument, Article 33(4) in the European Commission's text foresees that the data controller *"shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations"*. In this regard, consultation with all relevant stakeholders demonstrates the flexibility of the DPIA tool to evolve and adapt to concerns of individuals⁴⁰.

Therefore, the provision of Article 33 in the European Commission's version seems to replace and improve the general notification obligation which is stipulated in Article 20 of the DPD. In this respect, Article 20 of the DPD seems to function as a forerunner to the DPIA obligation stipulated in Article 33 in the European Commission's proposal for a GDPR and which, in essence, establishes the obligation for controllers and processors to conduct a risk analysis from the outset of any processing operations likely to present specific risks to the rights and freedoms of data subjects⁴¹.

After briefly examining how the Commission's draft of the GDPR deals with DPIAs, we now consider how the Parliament's draft of the GDPR deals with the concept in its draft of the GDPR, before turning to the Council's perspective on DPIAs.

2.3 The Parliament on the proposed GDPR

The European Parliament would introduce, in its first reading⁴², a new obligation for controller, or the processor where applicable, to *"carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks"* (art 32a(1) in the European Parliament's version). According to the outcome of the European Parliament's first reading⁴³, data controllers and/or processors are obliged to perform a risk analysis in order to identify the potential impact of the intended data processing operations on the rights and freedoms of the data subjects when specific risks arise⁴⁴. This risk analysis seems to be a precondition if data controllers/processors want to go through processing operations, which are likely to present specific risks. As a result, a DPIA would be performed depending on the results of such risk analysis.

³⁹Wright D., Finn R., Rodrigues R., *"A Comparative Analysis of Privacy Impact Assessment in Six Countries"*, Journal of Contemporary European Research, 2013, 9 (1), pp. 160-180.

⁴⁰Wright D., Wadhwa K., *"Introducing Privacy Impact Assessment Policy in the EU Member States"*, International Data Privacy Law, 2013, Vol. 3, No. 1, pp 13-28.

⁴¹Hon K.W., Kosta E., Millard C., Stefanatou D., *"Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation"*, Tilburg Law School Legal Studies Research Paper Series No. 07/2014 available at: <http://ssrn.com/abstract=2405971> p 29-30.

⁴²Proposal 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) - Outcome of the European Parliament's first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at <<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>>.

⁴³Proposal 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) - Outcome of the European Parliament's first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at <<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>>.

⁴⁴Hon K.W., Kosta E., Millard C., Stefanatou D., *"Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation"*, Tilburg Law School Legal Studies Research Paper Series No. 07/2014 available at: <http://ssrn.com/abstract=2405971> p 30.

In this context, the approach followed by the European Parliament seems to be more rigorous compared to the Commission's proposal. In particular, the inclusion of the new Article 32a – titled “*Respect to Risk*” – under the European Parliament's amendments⁴⁵ provides for a thorough delineation on the necessary preconditions in order for the data protection framework to be ensured. In this respect, it seems that the European Parliament tries to establish a more analytical and concrete framework with respect to privacy and data protection aiming at a transparent, secure and safe processing environment for privacy and data protection rights of data subjects.

Under this point of view, a list of processing operations is provided in Article 32a(2) in the European Parliament's version. In particular, it is stipulated that the following processing operations are likely to present specific risks:

- a) *processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;*
- b) *processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;*
- c) *profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;*
- d) *processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*
- e) *automated monitoring of publicly accessible areas on a large scale;*
- f) *other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);*
- g) *where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;*
- h) *the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;*
- i) *where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.*

This list, albeit seemingly more thorough and detailed in comparison with the one provided in Article 33(2) of the European Commission's proposal for a GDPR⁴⁶, still remains an indicative one. This is evident due to the use of the word “*likely*” in the European Parliament's first reading, which seems to replace the word “*in particular*” in the European Commission's proposal. In this respect, the quantitatively defined criterion stipulated in article 32a(2)(a) of the European Parliament's text constitutes merely an indicator as regards the extent of potential risk in the event of a data breach, notably given the fact that a merely numerical factor cannot be considered, from a legal perspective, as a de facto threshold with regard to risk.

However, article 32a(3)(c), in the European Parliament's version, enshrines the obligation of data controllers to carry out a risk analysis along with a DPIA for the processing operations which are referred in points (a) to (h) of the second paragraph of Article 32a⁴⁷. In this context, the European Parliament introduces, in its first reading, a privacy risk impact analysis model which foresees a two-step process. The first step refers to “*a set of questions necessary to help designers refine their understanding of the problem space*”⁴⁸ (privacy risk analysis). The second step involves a process necessary for managing potential privacy risks by “*categorizing, prioritizing and developing the relevant interaction techniques*”

⁴⁵Amendment 127- Proposal for a Regulation, Article 32a of the 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) - Outcome of the European Parliament's first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>.

⁴⁶Hon K.W, Kosta E., Millard C, Stefanatou D., “*Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation*”, Tilburg Law School Legal Studies Research Paper Series No. 07/2014 available at: <http://ssrn.com/abstract=2405971> p 30.

⁴⁷Hon K.W, Kosta E., Millard C, Stefanatou D., “*Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation*”, Tilburg Law School Legal Studies Research Paper Series No. 07/2014 available at: <http://ssrn.com/abstract=2405971>, p 30.

⁴⁸Abie H and Borking J., “*Risk Analysis Methods and Practices, Privacy Risk Analysis Methodology*”, DART/05/2012, Norsk Regnesentral Norwegian Computing Centre, p. 22.

and strategies” (privacy risk management)⁴⁹. In this respect, the risk-based model which is proposed by the European Parliament intends to introduce a management process of the protection of personal data, part of which is the DPIA mechanism.

Furthermore, while the European Commission’s proposal for GDPR provides in Article 33(3) the minimum requirements, which a DPIA shall cover (see Section 1.2), the European Parliament would complement and amend this provision⁵⁰. In particular, Article 33(3) of the European Parliament’s first reading stipulates that a DPIA shall contain at least the following:

- a) *“a systematic description of the envisaged processing operations, the purposes of the processing and, if applicable, the legitimate interests pursued by the controller,*
- b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
- c) *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,*
- d) *a description of the measures envisaged to address the risks and minimize the volume of personal data which is processed,*
- e) *a list of safeguards, security measures and mechanisms to ensure the protection of personal data, such as pseudonymisation, and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned;*
- f) *a general indication of the time limits for erasure of the different categories of data;*
- g) *an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;*
- h) *a list of the recipients or categories of recipients of the personal data;*
- i) *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, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;*
- j) *an assessment of the context of the data processing.”*

Compared to the respective provision (Article 33(3)) in the European Commission’s text, the European Parliament would introduce (in its first reading version), a more extensive list with regard to the minimum requirements which a DPIA shall contain. In particular, it seems that the European Parliament places more emphasis on the significance of the entire lifecycle management of personal data from collection to processing to deletion⁵¹, and, hence, it broadens the spectrum of the minimum components which a DPIA shall contain. Contrariwise, these components are only briefly mentioned in the European Commission’s text. In this respect, it seems that the European Parliament adopts a more proactive stance towards the DPIAs.

In essence, the European Parliament tries to provide a more solid framework with regard to the necessary elements which shall be included in a DPIA in order for information flows and risks to be identified and managed promptly. Namely, the European Parliament endeavours to include in the DPIA process specific elements such as the types of information collected, the reasons and purposes for its collection and processing, the conditions and safeguards which are in place, *et cetera*⁵². Recital 71a reflects the European Parliament’s approach with regard to the significance of DPIAs in the development

⁴⁹Abie H and Borking J., *“Risk Analysis Methods and Practices, Privacy Risk Analysis Methodology”*, DART/05/2012, Norsk Regnesentral Norwegian Computing Centre, p. 22.

⁵⁰Amendment 129- Proposal for a Regulation, Article 33(3) of the 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) - Outcome of the European Parliament’s first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014, available at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>.

⁵¹Amendment 129- Proposal for a Regulation, Article 33(3) of the 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) - Outcome of the European Parliament’s first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>.

⁵²Wright D., Finn R., Rodrigues R., *“A Comparative Analysis of Privacy Impact Assessment in Six Countries”*, Journal of Contemporary European Research, 2013, 9 (1), pp. 160-180.

of a sustainable data protection framework by stating that “*if impact assessments are thorough, the likelihood of any data breach or privacy-intrusive operation can be fundamentally limited*”⁵³.

Under this perspective, the European Parliament tries to integrate DPIAs to the overall approach to risk assessment and management, provided that DPIAs have the flexibility to evolve and adapt to particularities of any project throughout its life cycle process⁵⁴. In particular, the European Parliament seems to recognize that DPIAs can be used as a tool in order to identify any possible risks from the outset of any processing operation⁵⁵: in this respect, DPIAs are closely related to the concept of risk, given that they can contribute in identifying and managing risks potentially intrusive to the protection of personal data on a very early stage, even before any processing operations start.

Indeed, conducting a DPIA entails several benefits. For instance, unnecessary costs can be avoided, given that taking into consideration potential risks from the outset of any processing operations is more effective than trying to manage them at a later stage⁵⁶. Particular, devising solutions in order to encounter potential risks in the due course of any processing operations may, eventually, induce significant changes or even result in the cancellation of a flawed project, and, thus, corroborate a non-efficient allocation of costs⁵⁷. In this respect, the involvement and participation of all stakeholders may contribute to taking into consideration ideas which may not have been previously considered⁵⁸ and, in essence, abridge any conflicting interests. This means that the input of all stakeholders may result in a well-organised and well-developed project, due to the different perspectives involved⁵⁹. Thus, companies/organisations can be enabled to identify and manage potential risks for privacy and data protection of individuals in advance and, therefore, enhance their trust and reputation⁶⁰.

In this context, the purpose of adopting, at least at some degree, a risk-based approach, as it has been proposed by the European Parliament, seems to contribute to a better identification of the concept of risk as a key element in the DPIA process. Risk identification can result in better allocation of resources in a manner which does not violate the privacy rights of data subjects provided that greater risks are dealing with highest attention⁶¹. In this respect, the risk-based approach seems to comprise the appropriate solution in order for an overall management of the concept of risk to be applied in a data protection context. This is evident given the fact that this approach is capable of taking into consideration the different tiers of risk, which may jeopardize the protection of personal data.

However, the determination of the concept of risk in a legal context is not an easy task, particularly given the lack of a universal methodology on the application of a risk-based approach. Instead, the value of

⁵³Amendment 44- Proposal for a Regulation, Recital 71a of the 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) - Outcome of the European Parliament's first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at

<<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>>.

⁵⁴Wright D, De Hert P (eds), “*Privacy Impact Assessment*”, Law, Governance and Technology Series, Volume 6, Springer, p. 10-15.

⁵⁵SEC(2012) 72 final, Commission Staff Working Paper, “*Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*”, Brussels, 25.1.2012, Annex 6, p. 121-123 available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

⁵⁶Wright D., “*Should Privacy Impact Assessments be Mandatory?*”, Communications of the ACM, 2011, Vol. 54 No. 8, p. 121-131.

⁵⁷Wright D., “*Should Privacy Impact Assessments be Mandatory?*”, Communications of the ACM, 2011, Vol. 54 No. 8, p. 121-131.

⁵⁸Wright D., De Hert P. (eds), “*Privacy Impact Assessment*”, Law, Governance and Technology Series, Volume 6, Springer, p. 16-17.

⁵⁹Wright D., “*Should Privacy Impact Assessments be Mandatory?*”, Communications of the ACM, 2011, Vol. 54 No. 8, p. 121-131.

⁶⁰Wright D., “*Should Privacy Impact Assessments be Mandatory?*”, Communications of the ACM, 2011, Vol. 54 No. 8, p. 121-131.

⁶¹Financial Action Task Force-Groupe d'action financière, “*RBA Guidance For Legal Professionals*”, FATF/OECD, 2008, para 18 p. 8 available at <<http://www.fatfgafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf>>.

such an approach can be assessed based on the proper determination of the concept of risk⁶². Yet, the main challenge in this determination process relates to the fact that it encompasses subjective elements. This means that all parties involved are usually influenced by their own personal knowledge and expertise, which results in a subsequent subjective balancing of *risk* where persons may over-estimate it, but businesses may under-estimate it⁶³. As a result, a DPIA seems to obtain much more significance for individuals compared to businesses. In this respect, from a legal perspective, the seriousness of risk, as a pre-assessment step in the DPIA process, seems to be difficult to be determined or appraised in advance.

Therefore, the European Parliament would introduce Article 33a as an additional tool in order for the protection of personal data to be ensured. In particular, Article 33a (in the European Parliament's first reading version) stipulates the obligation of controllers and/or processors to carry out a compliance review, which shall demonstrate that the processing operations of personal data shall be performed pursuant to their original commitments as these commitments are reflected in the DPIA⁶⁴. Indeed, the compliance review shall be carried out no later than two years after carrying out a DPIA. As opposed to the European Commission's and European Council's (see below) texts, which do not provide for such a mechanism, the outcome of the European Parliament's first reading foresaw a new Article 33a entirely devoted to data protection compliance review mechanism. In this context, Recital 74a affirms the significance of periodic assessments and checks as an assurance tool with regard to the compliance of controllers and/or processors. In this respect, the provision of Article 33a of European Parliament's first reading seems to ascertain the full data protection management lifecycle idea, given that reviews or recommendations which are made throughout the lifecycle of the process can contribute to addressing and reinstating any inconsistencies in compliance.

After this brief account on the Parliament's approach towards DPIAs in the GDPR, the next section will turn to the Council's amendments – as of now⁶⁵ unofficial.

2.4 The Council on the proposed GDPR

On March 2014, the European Parliament voted, in plenary session, the amendments to the proposed GDPR, grouped in the so-called Albrecht Report⁶⁶. Following the Parliament's approval⁶⁷, the position of the Council of the European Union on the European Parliament's first reading is currently on its way. This means that the Council of Ministers is expected to reach an agreement on the Draft GDPR. Hitherto, the Council's amendments under examination are suggested in the Draft no. 11028/2014 of the 30 June 2014⁶⁸. It should be noted that the aforementioned document is unofficial, which means that these amendments have not yet been agreed internally by the Council.

⁶²Financial Action Task Force-Groupe d'action financière, "RBA Guidance For Legal Professionals", FATF/OECD, 2008, para 23 p. 8 available at <<http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf>>.

⁶³Financial Action Task Force-Groupe d'action financière, "RBA Guidance For Legal Professionals", FATF/OECD, 2008, para 31-33 p.10 available at <<http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf>>.

⁶⁴Amendment 130- Proposal for a Regulation, Article 33a of the 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) - Outcome of the European Parliament's first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at <<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>>

⁶⁵ Deliverable D:C-6.2 Prototype for the data protection impact assessment tool takes into account all legislative developments until 30.09.2014.

⁶⁶Named after the main Rapporteur for the Regulation in the European Parliament, Jan Philipp Albrecht. The Draft Report of the Committee on Civil Liberties, Justice and Home Affairs (LIBE draft report) 2012/0011 (COD) dated 17 December 2012 is available at <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf>.

⁶⁷Proposal 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) - Outcome of the European Parliament's first reading, Strasbourg, 10 to 13 March 2014, Interinstitutional File: 2012/0011 (COD), 7427/1/14 REV 1, Brussels, 27 March 2014 available at <<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%207427%202014%20REV%201>>.

⁶⁸Unofficial Council Document no. 11028/14 available at <<http://www.statewatch.org/news/2014/jul/eu-council-dp-reg-11028-14.pdf>>.

The Council seems to recognise as well the great significance of the concept of risk within the data protection framework. In particular, the Council would introduce the obligation for the controller to carry out a DPIA in case of the existence of specific risks⁶⁹. An indicative list of these risks is included in Recital 60 and covers, among others, processing operations which give rise to discrimination, identity theft or fraud, financial loss, damage of reputation, loss of confidentiality of data protected by professional secrecy, or any other significant economic or social disadvantage, or even any data processing which could lead to potential deprivation of the data subject's rights and freedoms⁷⁰.

Conversely, the main differentiation introduced by the Council's draft compared to the outcome of the European Parliament's first reading is that it would suggest that the list of the processing operations presenting specific risks stipulated in Article 33 in the European Commission's version is to become an exhaustive one, covering solely decisions with regard to profiling, sensitive data, public monitoring on a large scale and biometric and genetic systems on large scales⁷¹. In this respect, the carrying out of a DPIA would become mandatory *only* for the controller – not for the processor, as opposed to the European Commission's proposal and the European Parliament's first reading - in order for the outcome of the assessment to be taken into account as a means to demonstrate their compliance to data protection requirements (new Rec 64a).

The provision of an exhaustive list of risks could not be considered to be in line with Recital 71a in the European Parliament's first reading, which stipulates the establishment of a *sustainable data protection framework*. Risk cannot be considered as a pre-determined concept given that it encompasses not only subjective elements (see above), but it also partially incorporates the notion of likelihood, which can both render the association of risk with a specific list of processing operations fairly limited. Moreover, from a human rights perspective, an exhaustive list of risky operations narrows down the scope of assessment of other risks to the rights and freedoms of data subjects. This means that the pre-determination of the risky processing operations to particular circumstances can subsequently lead to an eliminated scope of DPIA jeopardizing the accountability of data controllers.

Arguably, the Council's proposed list of processing operations that present specific risks seems to incorporate some important elements. However, the adoption of such an exhaustive list seems to acquire an evaluative connotation which may supplant the significance of other risks, which may also threaten or compromise the protection of personal data. Under this framework, the risk as a key component of the DPIA seems to be deprived of its value given that the scope of understanding of its likelihood and severity are eliminated.

However, the rationale behind the Council's approach seems to derive from an attempt to bate potential financial burdens for controllers. According to the Commission's Impact Assessment for the data protection reform package, the costs for a small-scale DPIA can reach the amount of 14.000€, while for a full-scale DPIA can reach up to the amount of 149.000€⁷². Therefore, the Council would consider that the provision of an indicative list of risky processing operations, instead of an exhaustive one, along with the inclusion of a mandatory DPIA process would entail burdensome implications for micro, small and medium enterprises (Recital 76). In this respect, Member States seem to partially concur with the statement of Article 29 Data Protection Working Party (A29WP) that the adoption of the relevant obligations should be in tiers⁷³. Nevertheless, while the A29WP has not issued yet an opinion or

⁶⁹See Recital 60a

⁷⁰Recital 60 of the Council's unofficial Document no. 11028/14 available at <<http://www.statwatch.org/news/2014/jul/eu-council-dp-reg-11028-14.pdf>>.

⁷¹Council Document no. 5880/14, "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) - Data Protection Impact and Prior Checks", Interinstitutional File: 2012/0011 (COD) Brussels, 31 January 2014.

⁷² SEC(2012) 72 final, Commission Staff Working Paper, "Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", Brussels, 25.1.2012, Annex 6, p. 124-127 available at <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf>.

⁷³Article 29 Data Protection Working Party "Statement of the Working Party on current discussions regarding the data protection reform package" available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130227_statement_dp_reform_package_en.pdf>.

statement with regard to the adoption of a uniform approach towards DPIA mechanisms⁷⁴, it has indicated in a Statement on the role of a risk-based approach in data protection legal frameworks that the size of a company or an organization is irrelevant in order for the same level of protection of personal data to be guaranteed⁷⁵. In this context, the approach adopted by the A29WP is in line with EDPS's opinion on the data protection reform package, according to which, operations relating to processing of personal data entail specific risks for data subjects regardless of the size of a company⁷⁶.

Arguably, each small and medium enterprise ('SME') deals with different types of activities, which subsequently entail different implications and risks for the rights of data subjects. In this respect, the particularities of each company and/or organisation should be taken into consideration in order for the protection of personal data not to be compromised. Yet, SMEs are the backbone of the European economy given that they represent 99% of all European businesses⁷⁷. Under this framework, the adoption of a special provision as regards SMEs and their exclusion from an obligation to carry out a risk analysis or a DPIA would in fact exclude the majority of them. However, the Council's approach is somehow self-evident provided that it is consisted of the Heads of State or Government of the Member States and, thus, it adopts a more political orientation compared to the European Parliament, which is more protective towards the rights of the European citizens.

2.5 Conclusion

While the European Commission's proposed reform of the European data protection framework set the basis for institutionalization of the DPIAs, under the light of the outcome of the European Parliament's first reading, there is a trend not only to make them compulsory, but also to incorporate the concept of risk into the DPIA process (Article 32a in European Parliament's version).

This approach seems to enhance the scope of the DPIA mechanism in order to mandate data controllers to carry out a DPIA in those cases which are likely present specific risks to the rights and freedoms of data subjects. This means that the concept of risk is embedded in the DPIA process as a pre-assessment stage. Under this framework, a risk analysis would be able to function as an awareness methodology in order for a DPIA to be carried out. Therefore, DPIA seems to perform a dual function: on the one hand, it can serve as an accountability mechanism, where data breaches or losses occur⁷⁸,

⁷⁴According to Article 29 of the 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 (O.J. L 281, 23/11/1995 P. 0031 – 0050), the A29WP acquires independent action and advisory status. However, the A29WP's opinions are highly influential (See: Hon K.W, Kosta E., Millard C, Stefanatou D., "Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation", Tilburg Law School Legal Studies Research Paper Series No. 07/2014 available at: <<http://ssrn.com/abstract=2405971>> p 4-5) given that, according to Article 46(g) of the Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, "the European Data Protection Supervisor shall participate in the activities of the Working Party on the Protection of Individuals with regard to the processing of Personal Data set up by Article 29 of Directive 95/46/EC" (Article 46(g) of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L8/1).

⁷⁵WP 218, Article 29 Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks" adopted on 30 May 2014, p. 2, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> .

⁷⁶Opinion of the European Data Protection Supervisor on the data protection reform package, 2012, paras 81, 201, 205.

⁷⁷European Commission, *Fact and figures about the EU's Small and Medium Enterprise (SME)* available at <http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/index_en.htm> last accessed on 15 July 2014.

⁷⁸Wright D., "Should Privacy Impact Assessments be Mandatory?", Communications of the ACM, Vol. 54 No. 8, p. 121-131.

while, on the other hand, it can serve as a means to ensure effective protection of privacy and data protection rights⁷⁹, where privacy intrusive projects and services are to be performed⁸⁰.

Hence, the concept of risk seems to gain more and more ground in the data protection framework within the European Union. Indeed, the A29WP in its *“Statement on the role of a risk-based approach in data protection legal frameworks”*⁸¹ advocates in favour of the adoption of risk-based approach in a data protection legal framework. However, the A29WP does not consider the risk-based approach as an alternative to the already existing data protection rights and practices⁸². Instead, it seems to consider it as a complementary tool to the already existing privacy regulatory framework⁸³, given that data protection is a fundamental right protected under the EU Charter as such. In this respect, it is considered that the “rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved”⁸⁴. This means that the existence of risk to the privacy rights of data subjects is enough to trigger a risk analysis, which can be used as a calibration tool in order to ensure controllers’ accountability and compliance.

Nonetheless, one should keep in mind that risk is a concept which can be used in different contexts, since it has the potential to embed different modalities⁸⁵. Therefore, the so-called risk-based approach is not to be considered as a one-dimensional concept. On the contrary, the risk-based model is far away from a box-ticking exercise, which can influence inadvertently the substantial outcome of the process. Instead, this approach entails a dynamic and a momentum via which any potential vulnerability or threat, which may arise, develop or evolve at any time of the process, can constantly be assessed⁸⁶.

In this context, the merits of embedding the concept of risk, consistent to the European Parliament’s first reading, in a privacy context focus particularly to its potential to adapt to any potential hazard. In this respect, the risk-based approach seems to represent the decisive option on implementing and ensuring compliance, since it provides the baseline for improving the effectiveness of privacy requirements in practice⁸⁷.

Nevertheless, risk cannot be eliminated entirely, given that privacy cannot be considered as an absolute value⁸⁸. Besides, determining the level of risk at an early stage is often difficult, since it encompasses a versatile momentum which can be changed significantly throughout data processing procedures. The core consideration in this case is to balance the rights at stake on a case-by-case basis provided that all required procedures for the implementation of an impact assessment of privacy risks have been applied. In this regard, controllers are to be held liable in the event of not complying with data processing

⁷⁹SEC(2012) 72 final, Commission Staff Working Paper, *“Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data”*, Brussels, 25.1.2012, p. 81 available at <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf>.

⁸⁰Wright D., *“Should Privacy Impact Assessments be Mandatory?”*, Communications of the ACM, Vol. 54 No. 8, p. 121-131.

⁸¹WP 218, Article 29 Working Party, *“Statement on the role of a risk-based approach in data protection legal frameworks”* adopted on 30 May 2014, available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

⁸²WP 218, Article 29 Working Party, *“Statement on the role of a risk-based approach in data protection legal frameworks”* adopted on 30 May 2014, p. 2 available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

⁸³Centre for Information Policy Leadership, Hunton & Williams LLP, *“A Risk-based Approach to Privacy?”* An Initial Issues Paper for Privacy Risk Framework and Risk-based Approach to Privacy Project Workshop I Paris, France 20 March 2014, par. 20, p 5.

⁸⁴WP 218, Article 29 Working Party, *“Statement on the role of a risk-based approach in data protection legal frameworks”* adopted on 30 May 2014, para 1-2, p. 3 available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

⁸⁵DIGITALEUROPE, *“Comments on Risk-based Approach”*, 2013, p 2.

⁸⁶Financial Action Task Force-Groupe d'action financière, *“RBA Guidance For Legal Professionals”*, FATF/OECD, 2008, para 20 p. 8 available at <<http://www.fatf-gafi.org/media/fatf/documents/reports/RBA%20Legal%20professions.pdf>> .

⁸⁷Centre for Information Policy Leadership, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* p 2.

⁸⁸Centre for Information Policy Leadership, Hunton & Williams LLP, *“A Risk-based Approach to Privacy?”* An Initial Issues Paper for Privacy Risk Framework and Risk-based Approach to Privacy Project Workshop I Paris, France 20 March 2014, par. 18, p. 4.

requirements or of inability to demonstrate such compliance (Rec 60 European Commission's Proposal). Indeed, the European Parliament and the European Council seem to affirm such an approach given that they both make a direct reference to the value of carrying out an impact assessment as a means to demonstrate compliance.

Accordingly, the capability of a risk-based approach to embed different modalities allows for a more effective and flexible data protection framework structured in such a manner that could deal with technological advancements⁸⁹. In this respect, if DPIAs are integrated in the overall approach to risk management⁹⁰, they can provide a sustainable and useful tool of identification of possible risks from the outset of any processing operations. Arguably, the costs, which are of great concern on behalf of the Council, that a mandatory DPIA may entail for a company/organisation, especially given that the European entrepreneurial landscape is consisted, in its majority, of SMEs, are of significant importance. However, the extent and magnitude of data breaches (consider, for instance, the aftermath of *DigiNotar* case⁹¹), notably in terms of trust to the online interactions, seem to levy greater financial burdens to the SMEs. In this respect it seems to be preferable for the European legislator to mandate a preliminary assessment of the risks on the privacy rights of data subjects, and contingent upon to its results, to impose a compulsory DPIA adapted to the nature and scale of the project⁹². The creation of the DPIA Questionnaires, the discussion of which follows in the section below takes into account the legal requirements discussed.

⁸⁹Digital Europe 28 Aug 2013, DIGITALEUROPE Comments on Risk-based Approach, p 2.

⁹⁰Wright D., "Should Privacy Impact Assessments be Mandatory?", Communications of the ACM, Vol. 54 No. 8, p. 121-131.

⁹¹*DigiNotar* was a digital Certification Authority (CA) whose systems were hacked in mid July 2011. For two months (until late August) hundreds of rogue certificates were issued. The incident was not reported by the CA itself, but instead a notification report was sent by a German sister organisation to the Dutch CERT Govcert.nl. The forensic report revealed that, albeit *DigiNotar* was in compliance with ETSI standards and yearly audits, the implemented security practices were poor setting at risk the data of hundreds of users (See: Arnbak, Axel and van Eijk, Nico, "Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain" (August 15, 2012). 2012 TRPC. Available at SSRN: <<http://ssrn.com/abstract=2031409>> or <<http://dx.doi.org/10.2139/ssrn.2031409>>.

⁹²Wright D., "Should Privacy Impact Assessments be Mandatory?", Communications of the ACM, Vol. 54 No. 8, p. 121-131.

3 DPIA questionnaires

The proposed GPDR provides for a series of accountability measures aiming at ensuring effective protection of personal data. Data Protection Impact Assessments (DPIAs) fall under the scope of those measures, aiming at mitigating risks resulting from certain processing operations (See, also, Section 2). In practice, a DPIA screening consists of a set of questions allowing for multiple choice or free text answers, which help to assess the risks for personal data involved in the intended processing. Taking into account the above, as well as the various examples of existing DPIAs, the section below proposes a DPIA questionnaire tailor-made to address particular data protection risks associated with cloud computing services.

The DPIA questionnaire is part of the DPIA tool and will appear on the tool's user interface (See, Section 5.1.1). The user of the DPIA tool who will be requested to fill in the questionnaire will not necessarily be an expert. The questions are, therefore, formulated in an understandable language for ordinary users, in order to facilitate them in providing the right information⁹³. Note that the individual users of the DPIA tool will be acting either on behalf of a Small and Medium Enterprise (SME) or in their own capacity.

The discussion in Section 3.2 explains the methodology that was adopted in order to create the DPIA Questionnaire; a detailed listing of the sources used throughout the creation of the DPIA questionnaire is included. Section 3.3 explains the structure of the DPIA tool as a whole. There are in fact two questionnaires involved in utilising the DPIA. The first questionnaire is a pre-screening assessment which must be carried out in order to understand whether going through the main DPIA assessment is necessary or not. The second questionnaire is an additional set of questions that need to be answered by the user in order to conduct the full-scale DPIA assessment. Finally, in section 3.4 there is an extended discussion about the reasoning and the purpose behind the structure of the DPIA questionnaire.

3.1 Methodology

Given that the current European data protection framework is under review and that the proposed GPDR is under scrutiny, we had to decide whether the questionnaires would take into account new developments proposed within the GDPR, notwithstanding the fact that the proposed GDPR is not hard law at this point. Following discussions within the A4cloud consortium, all partners agreed that the DPIA tool should be future proof⁹⁴ and therefore we took into account both the Data Protection Directive (DPD)⁹⁵, as it is still the main European data protection framework, and the upcoming GDPR⁹⁶, rather than focusing exclusively on the legislation currently in vigour. The aim we set was to develop a tool that could be used effectively under both regimes.

Taking into account that the DPD does not explicitly mandate the utilisation of DPIAs, but allows for such assessments to be performed, the Directive served as the basis, or a starting point, for creating an appropriate DPIA tool. In this respect, the DPD provided us with the current general data protection framework, while the GDPR functioned as a concrete guideline for the deployment of an up-to-date DPIA questionnaire. In particular, the principles relating to processing of personal data, such as the purpose limitation and data minimisation principles, derived from the DPD, whereas, for example, the conditions under which a DPIA would be performed derived from the GPDR.

⁹³ "(O)rganisations, businesses and individuals interested in utilising cloud computing products must ensure they are aware of the privacy and security risks associated with using the product and take those risks into account when deciding whether to use it. For anyone intending to use a cloud computing product on a commercial basis, or otherwise to store other individuals' personal information, this should involve undertaking a PIA before adopting cloud computing techniques": Svantesson, Dan, and Roger Clarke. "Privacy and consumer risks in cloud computing", Computer Law & Security Review 26.4 (2010): 392.

⁹⁴ For more on the concept of "future-proof" see under section 3.4: Discussion.

⁹⁵ 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 [1995] OJ L281/31 (DPD).

⁹⁶ Which will arguably embody the current state of the art in data protection legislation, as well as the result of the doctrinal elaboration the concept had in the last two decades.

The already existing literature⁹⁷ helped us understand in depth the theoretical background of the purposes of DPIAs, aligned with the European legislative texts and existing Privacy Impact Assessment (PIA) and DPIA models. In this respect, we were enabled to carve a clear understanding of the aims of a DPIA. Additionally, several DPIAs and PIAs models, produced mainly by national data protection authorities, proved helpful input as well. A thorough examination of existing PIA and DPIA models and guidelines⁹⁸ served as an illustration mechanism in order to develop our own tool, adapted to the particularities of European legislation.

The analysis of the DPD, GDPR, and various DPIA and PIA models are reflected in the construction of the questionnaire's framework⁹⁹: the legal norms and the PIA/DPIA models utilised¹⁰⁰ allowed us to develop the "Question" field (and the related "Explanation" one), while the sources on risks in cloud environments were used to give a logical structure to the questionnaire and to weight the answers provided by users. The "Answer" fields were developed to steer the user throughout the questionnaire according to a logic order that was formulated mainly through the examination of the DPD and the GDPR, while assessing the impact and the likelihood of an unwarranted event happening.

Particular emphasis was given to a series of documents (see section 3.5 below) regarding the most commonly occurring incidents in cloud ecosystems; from a data protection viewpoint, these incidents provided valuable insights on the cloud's potential threats to informational self-determination, on their likelihood and on their foreseen impact. We conceived risk, defined as the likelihood of an unwanted, negative event happening, as the by-product of the interplay between the likelihood of an event and of the impact that event would have. In this respect, we based the construction of the questionnaire on that conception, which is to say we used existing literature and reports to investigate, on one hand, the most harmful privacy-related incidents, and on the other the most likely ones, all in order to develop a better understanding of what to ask when assessing the impact of an undertaking's activities on data subjects' privacy and data protection rights. Since the questionnaire aims to assess, *grosso modo*, how and how much a cloud user's undertaking deviates or could deviate from the physiology dictated by data protection norms (DPD and of the most updated version of the upcoming one GDPR), and the impact of its activities on data subjects, it seemed proper to consider, amongst other prominent factors, the most likely and/or the most harmful incidents in cloud environments. The situations that are most likely to threaten individuals in the cloud or that, if happening, would harm them the most, provided a useful list of the risks whose impact and likelihood the DPIA tool aims to assess.

In terms of process, a first draft version of the questionnaire was created by making a synthesis of the legal requirements set forth by the legal texts mentioned previously and of the conclusions we reached, while reviewing the existing PIAs and DPIAs (see section 3.5 below). The first draft version went through another round of reviews, in order to receive feedback from all partners and further amend the questionnaire and render it appropriate to the cloud. Following several discussions over the regular teleconferences and input provided by all partners, the basic structure of the questionnaire was agreed, allowing for the further development of the DPIA tool's interface. Finally, the legal partners made a last review of the questionnaire, to polish minor inconsistencies regarding the terminology used and to improve the way certain questions were articulated.

The development of the questionnaire, as for the sources utilised, relied upon thorough research into legal texts, books, a number of articles and policy documents, as well as reports produced by European Institutions.

⁹⁷ e.g. Wright, David, and Paul De Hert, "Introduction to privacy impact assessment", Springer Netherlands, 2012; Wright, David, et al. "Privacy, trust and policy-making: Challenges and responses", Computer law & security review 25.1, 2009: 69-83; Clarke, Roger. "Privacy impact assessment: Its origins and development", Computer law & security review 25.2, 2009: 123-135; Wright, David. "The state of the art in privacy impact assessment", Computer law & security review 28.1, 2012: 54-61; Warren, Adam, et al. "Privacy Impact Assessments: International experience as a basis for UK Guidance", Computer Law & Security Review 24.3, 2008: 233-242; Wright, David, "Should privacy impact assessments be mandatory?", Communications of the ACM 54.8, 2011: 121-131.

⁹⁸ For more information about the model PIAs and DPIAs we used see under section 3.5: Sources.

⁹⁹ The table we developed is composed by the following categories: question, explanation of the question, question type (which frames the possible answers to be given by the users, e.g. in the form of radio buttons, checkboxes, or yes/no binary answers), responses to be given to the users in order to educate them while they go through the questionnaire, actions to be performed by the tool as a consequence of the users' answers (e.g. go to the next question). A weighting of the users' activities' impact on data subjects' privacy and data protection was originally embedded in the table as well.

¹⁰⁰ See *supra* note 4.

In particular, Articles 6 and 7 of the current DPD proved to be valuable foundations for the formulation of certain questions of the questionnaire¹⁰¹. Moreover, the GDPR, as it has been formulated following the European Parliament's first reading, was used as the starting point for the development of the questionnaire. For both sections of the questionnaire (the so-called "pre-assessment" stage and the full-scale DPIA stage) we used Articles 32a and 33 of the outcome of the European Parliament's first reading on the GDPR as a basis (however the GDPR in its entirety was taken into account for the deployment of the DPIA tool).

In addition to this, David Wright and Paul De Hert's "Privacy Impact Assessment"¹⁰² served as a general starting guide on the Privacy Impact Assessment framework. The broad scope of this book with regard to the use and application of existing PIAs helped us understand the different approaches of DPIAs among different countries, as well as how to link the detected divergences in DPIAs to the current data protection trends. Therefore, we were enabled to establish a DPIA application as an organizational practice and not as merely a compliance checkbox tool.

ICO's "Conducting Privacy Impact Assessments: Code of Practice"¹⁰³, in conjunction with the Australian "Privacy Impact Assessment Guide" of the Office of the Australian Information Commissioner (OAIC)¹⁰⁴ also proved to be useful tools in phrasing particular questions¹⁰⁵. The ICO's PIA Handbook¹⁰⁶ constituted the key inspirational instrument in drafting the questions related to the grounds of processing.

Despite the existence of several PIA/DPIA models which deal with traditional cases of processing, there is hardly a sufficient number of cloud-tailored DPIA models, especially when considering the growing importance and pervasiveness of the cloud computing model in the modern digital economies and the fundamental differences that run between traditional IT environments and the cloud. However, notably, the Deliverable D1.2.4 "Cloud Computing - Data Protection Impact Assessment"¹⁰⁷ for the Tclouds project served as a solid basis for drafting cloud-relevant questions, especially for the full-scale DPIA questionnaire. Additionally, ENISA's "Cloud Computing: Benefits, risks and recommendations for Information Security"¹⁰⁸ constituted a helpful methodological tool in identifying and evaluating risks on the data protection rights. ENISA's report "cloud Security Incident Reporting: Framework for reporting about major cloud security incidents"¹⁰⁹ formed the key element for the development of the evaluation scheme we propose. Finally, Millard's ground-breaking text¹¹⁰ provided a comprehensive account of the law relevant to the cloud environment. Thus, it acted as a practical guide which was used to articulate the proper cloud-relevant questions¹¹¹, which can have an impact on ensuring how information relating to individuals is intended to be processed.

Several other scholarly publications have been consulted for targeted guidance on particular topics.

¹⁰¹ For instance, Question 9 ("Are all the information and its subsets you handle necessary to fulfill the purposes of your project?") or Question 16 ("Does your project involve the use of existing personal information for new purposes?") were drafted by taking into consideration the already existing legal requirements.

¹⁰² Wright, David, and De Hert, Paul *"Introduction to privacy impact assessment"*, Springer Netherlands, 2012.

¹⁰³ Information Commissioner's Office, *"Conducting privacy impact assessments code of practice"*, ICO, 2014.

¹⁰⁴ Australian Government, Office of the Australian Information Commissioner, "Privacy Impact Assessment Guide" (OAIC) (Reviewed in May 2010).

¹⁰⁵ For instance, question 10 ("Is it possible for the individual to restrict the purposes for which you process the information?").

¹⁰⁶ Information Commissioner's Office, "Privacy Impact Assessment Handbook", ICO, n.d. available at http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

¹⁰⁷ Marnau, Ninja, Jensen, Meiko, Schlehahn, Eva, Ferrer, Morte, Ricardo, Hansen, Marit, *"cloud Computing Data Protection Impact Assessment"*, D.1.2.4, Tclouds, 7th Framework Programme, 2013.

¹⁰⁸ European Network and Information Security Agency, *"cloud Computing Benefits, risks and recommendations for information security"*, ENISA, 2009.

¹⁰⁹ European Network and Information Security Agency *"cloud Security Incident Reporting: Framework for reporting about major cloud security incidents"*, ENISA, 2013.

¹¹⁰ Millard, Christopher J., ed. *"cloud Computing Law"*, Oxford University Press, 2013.

¹¹¹ For instance Questions 47-49 (Does the service provider that you use provide you just with raw computing resources, such as processing capacity or storage, for the information that you process? Does the service provider you use provide you with an environment or platform in which you can develop and deploy software? Does the service that you use consist of the provision of end user applications run by the cloud service provider?) which refer to the service models in a cloud environment.

3.2 Structure

The questionnaire, as it has been mentioned previously, is composed of two sets of questions. The first section constitutes the pre-assessment stage, while the second section, namely, the assessment stage, forms a fully-fledged DPIA. The first section is already a preliminary stage, which indicates whether a full DPIA would be necessary or recommended. For a consistent and accurate result, however, regarding the risks of particular processing operations, the completion of both questionnaires is necessitated.

The Pre-assessment stage

This pre-assessment stage includes a set of seven (7) questions. Its purpose is to enable users to identify whether the processing operations of their undertaking can be perceived as potentially risky to the protection of personal data of the individuals.

The pre-screening aims at providing an initial evaluation for the user of the DPIA tool. It initially assesses whether the information he deals with constitutes personal data or not, and then it evaluates the kind of information processed, its sensitivity, the purposes of the processing, the actors involved and the extent to which the information is likely to be diffused. Our purpose was mainly to provide the user with a very short and incisive pre-screening application to assess the presence or the absence of some general factors that indicate the use of sensitive information, e.g. the very qualification of personal data of the information dealt with by the tool's user¹¹², or the presence of sensitive data amongst it¹¹³.

In particular, the pre-assessment stage includes the following set of questions:

Data Protection Impact Assessment Screening Questions:

These questions are intended to help you decide whether a data protection impact assessment ('DPIA') is necessary. Giving determinate answers would be a clear indication that a DPIA would be a useful exercise for the tool user's undertaking, while others would indicate a compliant attitude. However, the answers to the screening questions need to be considered as a whole, in order to decide whether a full-scale DPIA is necessary or not.

Legal disclaimer:

No information or content displayed in this tool should be construed, interpreted or relied upon as constituting legal advice, or a recommendation in respect of taking any course of action to comply with data protection laws, or legal obligations of any kind, and within any jurisdiction to which the European data protection law applies. Nothing in this tool is intended to be an invitation or inducement to engage or enter into, or advice against engaging or entering into, an undertaking of any kind. The content or information displayed in this tool is for general informational purposes regarding compliance with the applicable data protection laws only. [Body who owns DPIA] shall not be liable for any damages resulting from the use of the tool, including damages caused by viruses or any incorrectness or incompleteness of information provided on the tool.

If you want more information about compliance with data protection laws in respect of the information you input into the tool, you will need to contact the relevant authorities.

¹¹² See pre-screening stage Question number 1.

¹¹³ See pre-screening stage Questions number 2 and 3.

1. Based on the information that you process, can you identify one or more individuals about whom you are processing information?

Explanation: Can the information used be associated to a particular customer or employee, either directly (e.g. by using names) or indirectly (e.g. by using license plates, social security number, addresses, telephone numbers or other information that you hold)?

- YES → the undertaking's activities constitute processing of personal data -> Question 2
- NO → No need to proceed. The information you process is not personal data under the EU law.

2. Does the information that you process reveal certain characteristics of individuals?

Explanation: Can you, or will you, use the information you process to qualify your customer or employee, for instance on the basis of (online) behavior, attendance, marital or social status, salary level, work performance, or zip code? If you build 'profiles' of individuals, answer yes to this question.

- YES
- NO

3. Do you deal with any kind of the following categories of information?

Explanation: the following categories of information are of a particularly sensitive nature, and need to be dealt with

- race or ethnic origin;
- political opinions;
- religion or philosophical beliefs;
- sexual orientation or gender identity;
- trade-union membership and activities;
- genetic or biometric data or data concerning health or sex life;
- administrative sanctions, judgments, criminal or suspected offences;
- data on children;
- data on employees;
- location data;
- data that can be used for identity theft, such as social security number, credit card information, passport or driving license data.

4. What is the scale of your processing operations?

Explanation: The scale includes, for instance, the number of persons to whom the information you deal with relates to, the amount and granularity of information per person or the number of people who have access to the information that you process.

- Large
- Medium
- Small
- I don't know
- Not applicable

5. Is the nature, scope and/or purpose of your business, profession or activity based on a regular and systematic monitoring either of any natural person(s) or of publicly accessible areas?

Explanation: Think, for instance, of virtual public areas, such as social networks or public fora.

- YES
- NO

6. How likely is that incidents will raise concerns amongst individuals and/or legal entities?

Explanation: Think of, for instance, data breaches, inaccurate, incomplete or outdated data related to the information that you process, use of data for purposes other than the ones for which they were collected

- Large
- Medium
- Small
- I don't know
- Not applicable

7. Are there any third parties involved in the storage, processing, use, or transfer of any information that you deal with?

Explanation: the interplay with third parties exponentially increases the risks deriving from processing activities.

- YES
- NO

The assessment stage

The second set of questions includes fifty-six (56) questions. The questions are grouped into five (5) topical areas¹¹⁴, which refer to: 1) the type of project, 2) the collection and use of data, 3) the project's storage and security policies, 4) data transfers, and 5) cloud specific issues. The aim of this set of questions is to assess in a more granular manner how the interactions between the subjects that perform the DPIA – individuals or SMEs – and CSPs impact data subjects' rights to privacy and data protection, and how the system is designed – if so – to prevent or mitigate the potential adverse outcomes of those interactions.

In order to do so, we devised an inquiry that targets the undertaking of the DPIA tool user, the data it processes, and the causal nexus between undertaking and the processing operations; we inquire, furthermore, about where and how the data is kept, and about the paths it might take, through more queries regarding storage, security and transfers of information. Because the cloud environment is significantly different from the traditional IT settings most individuals are accustomed to, a last group of questions was devised in order to adapt the rough DPIA model to the peculiarities of the particular environment in consideration.

In particular, the assessment stage includes the set of questions shown in Appendix 9.2.

3.3 Discussion

Under the GDPR, as it has been amended by the outcome of the European Parliament's first reading, there is a trend to make DPIAs compulsory when the processing operations of controllers are likely to present specific risks for rights and freedoms of data subjects (Article 32a of the Parliament's text Respect to Risk). This approach seems to confirm the importance of DPIAs to protect data subjects' rights and freedoms: this meant for us embedding in the DPIA process the concept of risk analysis introduced in the earlier stated Article 32a of the European Parliament's amended text.

In order to do the full scale DPIA assessment, one must first complete the pre-assessment questionnaire in order to establish whether he is prone to risk or not; in this respect, the main challenge when drafting these questions was to create a reliable and consistent concept of risk¹¹⁵. Under the framework we developed, the risk analysis conducted at the pre-assessment stage would be able to function as an awareness tool in order to alert (cloud) customers as to whether or not a DPIA needs to be carried out. The discussion will mainly focus on the assessment stage, though, because this stage constitutes the fundamental enabler for the deployment of a fully-fledged DPIA.

DPIAs perform a dual function: on the one hand, they can serve as an accountability mechanism, where data breaches and losses may occur¹¹⁶, while, on the other hand, they can serve as means to ensure effective protection of privacy and data protection rights¹¹⁷, where privacy intrusive projects and services are to be performed¹¹⁸.

Because of the multiplicity of data protection issues covered by the GDPR in conjunction with the complexity of the concept of personal data, we avoided open questions. Therefore, the majority of the questions we formulated are either YES or NO, checklist or radio button ones.

¹¹⁴ The key inspirational document which enabled the taxonomy of these topical areas was the document "Privacy Impact Assessment: Introductie, handreiking en vragenlijst" of NOREA – de beroepsorganisatie van IT-auditors (2013) available at

<http://www.norea.nl/readfile.aspx?ContentID=36650&ObjectID=343968&Type=1&File=0000040117_NOREA%20A4%20Privacy%20Impact%20Assessment%2003%20WEB.pdf>

¹¹⁵ As put forward by Article 32a of the GDPR in the European Parliament's first reading version.

¹¹⁶ Wright D., "Should Privacy Impact Assessments be Mandatory?", Communications of the ACM, Vol. 54 No. 8, p. 121-131

¹¹⁷ SEC(2012) 72 final, Commission Staff Working Paper, "Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", Brussels, 25.1.2012, p. 81 available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf.

¹¹⁸ Wright D., "Should Privacy Impact Assessments be Mandatory?", Communications of the ACM, Vol. 54 No. 8, p. 121-131

As to the first area of questions relating to the type of project undertaken by the tool's user, our aim was to frame, on one hand, the kind of activity performed by the CSP's client, and on the other, the aim of that activity. We considered the fact that a controller could handle personal data (for instance, the controller may obtain information such as the name, e-mail address, and bank details of users through online subscription forms that it deploys) for a number of different reasons and aims, such as, for instance, commercial purposes on one hand, or purposes of public interest in the area of public health on the other. Therefore, we decided to include two separate inquiries: one regarding the activities through which data is processed, and another regarding the very purpose of the processing.

The second area of questions regards the collection of the information, the usage that processors make of that information and the means with which personal data is handled (i.e. *how* personal data is handled). This section draws heavily from the basic principles of both the DPD and the GDPR. For instance, it assesses the existence of solid, legitimate grounds for processing, compliance with data protection principles such as for instance data minimization, and compliance with the rights of the data subject sanctioned by law.

Storage and Security (deletion included¹¹⁹), moreover, is considered a third area which deserves specific consideration, especially in relation to the particular traits of cloud Computing.

The investigation we propose was developed according to an "individual-centric approach", which tried to deepen the level of protection accorded to data subjects irrespectively of the subject (either CSPs or their customers) that exerts concrete control over the particular aspect considered: that is to say, we considered it more useful to ask individuals and SMEs questions pertaining to the CSPs' areas of control¹²⁰, accepting the chance they might not know the answer to our inquiry, rather than making sure to ask questions every undertaking is (or should be) able to answer in every instance. A major concern we had was related to the 'updatedness' of the information dealt with by the tool user. Through the valuable input of the partners whom reviewed the numerous drafts of the questionnaire, we decided to include two questions¹²¹ regarding the foreseen negative consequences of the outdated information processed by the tool user's undertaking; specifically the questionnaire addresses the consequences of outdated information about data individuals¹²² and how such outdated information can lead to regulatory liability¹²³. Whether or not outdated information may result in civil or criminal liability is not addressed, because it was not within the scope of the DPIA. An individual-centric approach has also been adopted for the fourth set of questions, which relates to the transfer of information, be it to third parties or to non-EU countries. This is because transferring information physiologically increases the risks that the data subjects are subject to. Furthermore, due to the target of the DPIA tool, this class of inquiries – albeit worded in a non-technical manner – caters for the possibility that the tool's user does not possess an adequate level of knowledge in order to provide satisfactory answers to all the questions posed. Much like with the third set of questions, we considered the possibility of a lack of answer better than avoiding inquiring on aspects of the cloud arrangements undertakings might be unaware of.

The final set of questions refers exclusively to cloud computing services. Given the complexities of cloud computing technology, it was a challenge – as stated earlier – how to formulate those questions in particular in an understandable language for an ordinary user. Each deployment model, for instance, has various ramifications which are not necessarily known in the first place to the user of the DPIA tool who is to decide whether to opt for a particular cloud computing service or not.

It is important for the users of a cloud service to know how to secure the information they process within the cloud environment. Taking that into account, the cloud relevant questions aim at ascertaining the level of exposure to risk that the user may have by virtue of using a specific type of cloud service. Two major aspects are important to establish in this regard. Firstly, it is important to know whether the cloud service used by the user of the DPIA tool is public, and thus shared with third parties, or private, and thus solely used by the user. Secondly, it is important to establish what the user utilises the cloud service

¹¹⁹ Note that deletion assumes particular importance in the cloud: the remoteness of the physical machines and the lack of control cloud users have over them, considered in relation to the fact that several different layers of deletion exist (from a mere drag-and-drop in the OS' virtual rubbish bin to the physical destruction of the hardware in which the virtual machine of the user lies), make deletion a focal point when assessing the risks a data subject is prone to.

¹²⁰ E.g. "Are measures in place to ensure an adequate level of security when the information is transferred outside of the EEA?".

¹²¹ Namely, Q 28: How severe would you deem the consequences of the information you process being outdated for the individuals it refers to? and Q 29: Would the fact that the information you process is not up to date expose you to any kind of regulatory liability?

¹²² Question 28, see *supra* footnote 19

¹²³ Question 29, see *supra* footnote 19

for. Three questions are relevant in determining this: Does the user utilise cloud in order to outsource all the IT infrastructure requirements it has (such as storage facilities, e-mail servers, etc.)? Does the user use the cloud in order to utilise one specific program or application? Or does the user use the cloud in order to develop software and applications?

Arguably, it is not expected that all users will be in the position to provide answers to the entire set of questions, given these are many and that certain¹²⁴ of them are quite specific. The user of the DPIA tool may proceed, though, without having answered all questions. However, if the user does not answer all questions, the final result will not be precise and, notably, the tool will not be able to provide a trustworthy suggestion on whether a DPIA is advisable or not. The output, therefore, would be incomplete, and consequently, the estimation of risks inaccurate. A progress bar to appear on the user's interface would inform the user with regard to the percentage of completion of the questionnaire.

The inclusion of a specific part of the questionnaire targeted only to the cloud environment serves as an enabler for the applicability of the DPIA tool to a non-cloud setting as well, ensuring that the DPIA Questionnaire remains future proof. In this sense, the tool adopts a technology-neutral approach, in order to avoid becoming soon outdated due to technological advancements. This approach can enable the application of the tool not only to the existing (and upcoming) legislation, but also to several other future Internet services. If this particular set of cloud-relevant questions is removed, the questionnaire can potentially be addressed to any SME (or individual acting in his own capacity), to be used in order to ensure compliance with the legal framework irrespective of whether the assessed undertaking operates in the cloud or not.

¹²⁴ For example: "Does the CSP have an insurance policy against the possible loss or compromise of the information you process in a cloud environment?"; "Does the CSP use resource isolation mechanisms in order to secure the information you entrust it?"

4 Cloud Adoption Risk Assessment Model

Building on the meta-model of cloud ecosystems introduced in the previous deliverable D36.1 this section presents a Cloud Adoption Risk Assessment Model (CARAM) for evaluating organizational, technical and security risks resulting from adoption of cloud solutions. The proposed Cloud Adoption Risk Assessment Model (CARAM) is complementary to the DPIA questionnaires presented in Section 3. It is designed to help cloud customers assess all kinds of risks that they face by selecting a specific cloud service provider, not only privacy-related.

CARAM is a qualitative deductive risk assessment model based on (ENISA, 2009) and Cloud Assessment Initiative Questionnaire (CAIQ)¹²⁵ (see D36.1 for a detailed introduction to these frameworks) that evaluates some background information obtained from cloud customers, cloud service providers and other public external sources, and assesses risk scenarios impacting cloud customers' assets (Cayirci et al 2014). It complements ENISA Risk Assessment Model by adapting it to specifics of CSPs and Cloud Service Consumers (CSCs) for a relative risk assessment.

We hope that it will facilitate cloud customers in making an informed decision in selecting the cloud service provider with the most preferable risk profile.

Figure 1 illustrates the CARAM process and data flow.

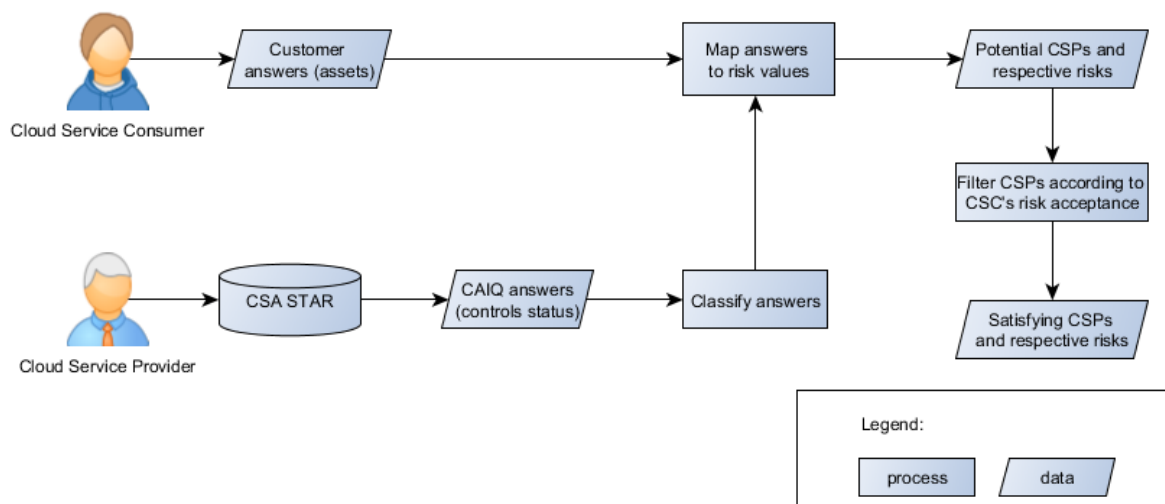


Figure 1 CARAM process and data flow

CARAM consists of the following blocks:

- A questionnaire for cloud customers (Section 4.1)
- A tool and an algorithm to classify CSP's answers to CAIQ to discrete values (Section 4.2)
- A model that maps the answers to both questionnaires to risk values (Section 4.1, 4.3)
- A multi-criteria decision approach with posterior articulation of cloud customer preferences for relative risk analysis (Section 4.4)

4.1 Risk Level Computation

ENISA identified in (ENISA, 2009) 35 incident scenarios that fall in one of the following four categories: policy and organizational, technical, legal and the other scenarios not specific to cloud computing (see Table 6). The likelihood of each of these scenarios and their business impact are determined in consultation with an expert group. The scale of probability and impact has five discrete classes between very low and very high. For example, the probability and impact of Incident Scenario P1 in "Policy and Organizational Scenarios" category (i.e., lock-in) are given as HIGH and MEDIUM relatively.

¹²⁵ <https://cloudsecurityalliance.org/research/cai/>

ENISA also provides a list of 53 vulnerabilities (i.e., 31 cloud specific and 22 not cloud specific vulnerabilities) and 23 classes of CSC assets that may be affected by the cloud adoption. Each of 35 incident scenarios is related with a subset of vulnerabilities and assets. For example, the Incident Scenario P1 is related to Vulnerabilities V13 (lack of standard technologies and solutions), V31 (lack of completeness and transparency in terms of use), V46 (poor provider selection), V47 (lack of supplier redundancy) and Assets A1 (company reputation), A5 (personal sensitive data), A6 (personal data), A7 (personal data critical), A9 (service delivery – real time services), A10 (service delivery).

The likelihood (probability) and business impact (impact) values that are determined by the experts are converted to the risk levels for each incident scenario based on a risk matrix with a scale between 0 and 8 as shown in Figure 1. Then, the risk levels are mapped to a qualitative scale as follows:

- Low risk: 0-2
- Medium: 3-5
- High: 6-8

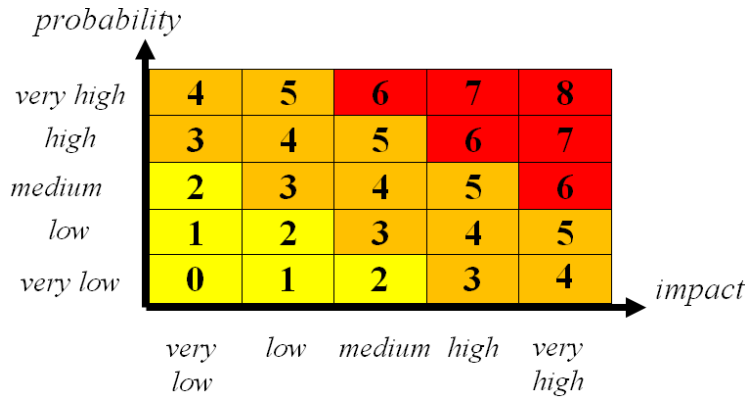


Figure 2 ENISA definition of risk levels

Hence, a cloud customer can assess the risk level related to an incident scenario qualitatively and understands what kind of vulnerabilities and assets are related to each scenario by examining (ENISA, 2009). These values represent educated guesses over a wide range of common cloud deployments and do not have a precise semantics. In practice, the risk levels are related to many factors such as the security controls that CSPs implement and the concerned assets of the specific users. Therefore, a generic value cannot be applied to all CSPs and CSCs. Although vulnerabilities and assets for each incident scenario are given by ENISA framework, it does not describe how those values can be adapted for a specific CSP and CSC pair. CARAM fills this gap. For that, first the qualitative scale used by ENISA as probability and impact values are mapped to a quantitative scale as follows:

- Very low → 1
- Low → 2
- Medium → 3
- High → 4
- Very high → 5

For example, probability P_1 and impact I_1 values for the first scenario (i.e., lock in) is HIGH and MEDIUM respectively. We map these values as follows: $P_1=4$ and $I_1=3$.

However, probability and impact of a risk scenario are very much dependent on the vulnerabilities and assets involved in. Therefore, these values cannot be the same for all CSPs and CSCs. CARAM adjusts the values from ENISA, taken as a baseline, considering additional information about the cloud service. For that, we use Equations 1 and 2:

$$\beta_i = P_i \times \vartheta_i \quad (1)$$

$$\delta_i = I_i \times \alpha_i \quad (2)$$

In Equation 1, for the risk scenario i , β_i is the adjusted probability, ϑ_i is the vulnerability index of a given CSP, δ_i is the adjusted impact and α_i is the asset index for a given CSC. Here we assume that probability and impact of an incident are proportional respectively to the number of non-addressed vulnerabilities by a CSP and the number of CSC assets related to risk scenario i . Note that vulnerability index of a CSP is the same for all CSCs and the asset index of a CSC is the same for all CSPs. Vulnerability and

asset indices are calculated as given in Equations 3 and 4 respectively, where v_{ki} is 1 if vulnerability k is in the list of vulnerabilities (ENISA, 2009) for risk scenario i , and 0 otherwise. Similarly, a_{ki} is 1 if asset k is in the list of assets (ENISA, 2009) for risk scenario i . Please note again that there are 53 vulnerabilities and 23 assets listed in (ENISA, 2009). The other two parameters ε_k and γ_k in Equation 3 and 4 are derived from the answers to the questionnaires for CSP and CSC (i.e., CAIQ and A4Cloud Questionnaire). The vulnerability related parameter ε_k is elaborated later in subsection 4.2. The asset related parameter γ_k is given value 0 if the CSC's answer to the question that "Does the service that you seek will involve any asset of yours that fall in the same category as asset k ?" is "No", and value 1 otherwise. We would like to highlight that CARAM is independent from the number of incident scenarios and probability, impact, vulnerability and assets assigned to the incident scenarios. Moreover, it is possible to assign weight values for each of assets and vulnerabilities if some of them are assumed as of higher importance comparing to the others.

$$\vartheta_i = \frac{\sum_{k=1}^{53} v_{ki} \times \varepsilon_k}{\sum_{k=1}^{53} v_{ki}} \quad (3)$$

$$\alpha_i = \frac{\sum_{k=1}^{23} a_{ki} \times \gamma_k}{\sum_{k=1}^{23} a_{ki}} \quad (4)$$

4.2 Control Implementation Data Collection

We use CSP's responses to CAIQ¹²⁶ to assign a value to the vulnerability related parameter ε_k (see Section 4.3). CAIQ aims at collecting data directly from CSP on how much they comply with the regulations/standards and how secure is their infrastructure. It consists of questions grouped into the control areas shown in Table 2, asking about the state of implementation. The CSPs are expected to answer these questions as "Yes", if the control is implemented and as "No" otherwise. However, most of the CSPs that have answered the questionnaire in STAR used free text explanations rather than simple "Yes" or "No", which is more informative but unsuitable for automated analysis. Table 1 shows example questions and answers on the Risk Management Program control area (RI-01) extracted from one of the CAIQ respondents:

Table 1 CAIQ example answers

RI-01.1	Is your organization insured by a 3rd party for losses?	The ISO Plan, Do, Check, Act process is used by the CSP to continually maintain and improve the risk management framework.
RI-01.2	Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?	"Establishing the ISMS and risk management framework" is covered under the ISO 27001 standards, specifically addressed in domain 4.2.1. For more information, we suggest a review of the publicly available ISO standards for which we are certified.

Albeit CSA has given clear guidelines to fill in the self-assessment, the provider preferred to refer to its certification, grouping the answers to the two questions in this control group. This makes it difficult for a consumer to interpret if the provider actually has these controls in place. Some human reader can understand the answer as positive, since the provider affirms to have risk management in place. On the other hand, other readers may perceive the answer above as an evasive explanation, meaning that the actual answer to the both questions is "No". Therefore, using the CIAQ in its current form means that there will always be some margin of error due to the human interpretation of the answers. CARAM provides the following mechanism to map the answers given to the questions in CAIQ to one of the categories in Table 2. Please note that the category "Yes" in Table 3 means the control is implemented, which is positive. The answer "Yes" to CAIQ questions do not always imply a more secure system (i.e., the control is implemented). For example, the "Yes" answer to CAIQ Question RS06-01 "Are any of your datacentres located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?" implies a negative outcome,

¹²⁶ <https://cloudsecurityalliance.org/star/self-assessment/>

which means the control is not implemented. Therefore, CARAM maps the answer “Yes” to this question as “No: the control is not implemented”.

Table 2 The control groups in CAIQ

1. Compliance	6. Legal
2. Data Governance	7. Operations Management
3. Facility Security	8. Risk Management
4. Human Resources Security	9. Release Management
5. Information Security	10. Resiliency
	11. Security Architecture

Table 3 The categorization of the answers given to the questions in the CAIQ

<ul style="list-style-type: none"> • Yes: the control is implemented • Yes, <i>conditionally</i>: the control can be implemented under some conditions • No: the control is not implemented • <i>Not available</i>: the answer is not given • <i>Not applicable</i>: the control is not applicable to the provided service

Given that there are about 100 of CSPs in the mentioned registry providing answer to about 200 questions each, the automation of this categorization could save significant time. For the automatic classification of the free text answers to CAIQ questions we use supervised machine learning algorithms provided by the WEKA tool¹²⁷. For that we have provided a training set representing a random sampling of around 300 classified answers out of overall circa 9000 answers and used it to classify the other remaining answers. The 10-folds cross-validation provided an accuracy of around 84% of correctly classified instances, which we consider enough for our purpose.

In this way we constituted the information base to be used in combination with the data on common threats and vulnerabilities in the cloud (e.g. from ENISA Cloud Computing Risk Assessment report) to estimate residual privacy risk levels (ENISA, 2009).

4.3 The Vulnerability Parameter for a CSP

After classification of the answers to one of the categories in Table 3, the implementation value q_m is assigned for each of the controls. If the answer to a question is “Yes”, that trivially means the control implied in question m is available (i.e., $q_m=0$) and hence the related vulnerabilities are mitigated. For “Not applicable” $q_m=0$: these controls do not impact the risk value. The “No” and “Not available” classes mean that the control will not be available, and therefore $q_m=1$. If the class is “Yes Conditionally”, the CSC needs to clarify with the CSP if the control can be implemented. If yes, $q_m=0$. Otherwise, $q_m=1$. When q_m is known for a CSP and a CSC, Equation 5 gives the vulnerability related parameter ε_k for the CSP and the CSC. Please note that this value is for a specific CSP and CSC pair.

$$\varepsilon_k = \frac{\sum_{m=1}^n r_{m,k} \times q_m}{\sum_{m=1}^n r_{m,k} \times b_m} \quad (5)$$

In Equation 5, n is the number of questions in CAIQ. $r_{m,k}$ is the mapping of the CAIQ questions to vulnerabilities: it is 1 if the question m is related to vulnerability k , and 0 otherwise. Our recommendation for this mapping is in Table 9 in Appendix 9.1.

Finally, $b_m=0$ if the answer to the question m is “Not Applicable” and 1 otherwise. This allows discarding the unrelated questions avoiding wrongly penalizing the CSPs.

In Equation 5 ε_k receives a minimum value 0 if all the controls related to the vulnerability k are implemented and hence the vulnerability does not impact negatively the risk values. The more controls

¹²⁷ <http://www.cs.waikato.ac.nz/ml/weka/>

related to the vulnerability k are not implemented, the higher ε_k is. Its maximum value is 1, which means the CSP has no measures against the vulnerability k .

4.4 Relative Risk Assessment with Posterior Articulation of CSC Preferences

ENISA Risk Assessment Model is based on 35 incident scenarios. This is too many in numbers for selecting a CSP that fits best to a CSC's requirements. Therefore, we first reduce the number of criteria from these 35 incident scenarios to three categories of cloud risks: risks to security, privacy and service (Cayirci, 2013). For that, we compute the probability that a privacy (β_r), a security (β_s) and a service (β_e) incident can occur and the impact of a privacy (δ_r), a security (δ_s) and a service (δ_e) incident by applying Equations 6 to 11. Table 10 in Appendix 9.1 provides a sample mapping of risk scenarios to these categories. In Equations 6 and 9, r_i is 1 if ENISA incident scenario i is related to privacy, and 0 otherwise (see Table 10). ω_{ri} and α_{ri} are real numbers between 0 and 1. They are the weight factors for probability and impact respectively. The significance of every scenario may not be the same when calculating an aggregated value for privacy, security and service incidents. Moreover, the scenarios may need to be treated differently for each CSC especially when calculating the aggregated impact values. The weight factors are for making these adjustments. If the significance of each scenario is the same, then the weight factors can be assigned 1. Similar to r_i , s_i and e_i are the mapping values for security and service risks respectively. ω_{si} and α_{si} are the weight factors for security scenarios, and ω_{ei} and α_{ei} are the weight factors for service scenarios.

$$\beta_r = \frac{\sum_{i=1}^{35} \beta_i \times r_i \times \omega_{ri}}{\sum_{i=1}^{35} r_i \times \omega_{ri}} \quad (6)$$

$$\beta_s = \frac{\sum_{i=1}^{35} \beta_i \times s_i \times \omega_{si}}{\sum_{i=1}^{35} s_i \times \omega_{si}} \quad (7)$$

$$\beta_e = \frac{\sum_{i=1}^{35} \beta_i \times e_i \times \omega_{ei}}{\sum_{i=1}^{35} e_i \times \omega_{ei}} \quad (8)$$

$$\delta_r = \frac{\sum_{i=1}^{35} \delta_i \times r_i \times \alpha_{ri}}{\sum_{i=1}^{35} r_i \times \alpha_{ri}} \quad (9)$$

$$\delta_s = \frac{\sum_{i=1}^{35} \delta_i \times s_i \times \alpha_{si}}{\sum_{i=1}^{35} s_i \times \alpha_{si}} \quad (10)$$

$$\delta_e = \frac{\sum_{i=1}^{35} \delta_i \times e_i \times \alpha_{ei}}{\sum_{i=1}^{35} e_i \times \alpha_{ei}} \quad (11)$$

When probability (i.e., β) and impact (i.e., δ) values are calculated, they are mapped to the qualitative scale as follows:

- [0, 1] → Very low
- (1, 2] → Low
- (2, 3] → Medium
- (3, 4] → High
- (4, 5] → Very high

Finally, by using the same approach as shown in Figure 2, the risk values for privacy R_r , security R_s and service R_e are obtained in a qualitative scale: Very Low < Low < Medium < High < Very High for each CSP-CSC pair. These three values are reported eventually to the user.

4.5 Limitations and Future Work

The accuracy of the risk assessment results using this method depends on the accuracy of the input data and the appropriateness of the proposed formulas. We believe that major sources of systematic errors are: 1) incorrect classification of the CAIQ answers; 2) vague CAIQ answers; and 3) ineffective

implementation of controls. The first and, to an extent, second errors may be estimated by the classification algorithm itself and appropriate statistical formulas for calculating the absolute error of a function of random variables. Addressing the last one would require additional methods for evaluating control effectiveness, e.g. penetration testing or analysis of previous incidents (see (Cayirci, 2013), (Habib, 2013) for example approaches).

Finally, we have implemented a Proof-of-Concept prototype to demonstrate CARAM as a part of the Data Protection Impact Assessment Tool (see Section 5) and used it to perform cloud adoption risk assessment of a use-case (see Section 6.1).

5 Data Protection Impact Assessment Tool

In order to demonstrate the data protection risk assessment approach proposed in Sections 3 and 4, we have developed the Data Protection Impact assessment tool (DPIAT).

The tool is used to identify what are the risks –related to data protection- for a given configuration and environment of carrying out a certain business transaction such as buying a new cloud service. The tool can be used by SMEs to show: how personal or sensitive the data is and how it can be secured in the cloud, and what risks there are with respect to data breaches and the privacy of cloud service users. Moreover, it provides insight to the potential threats while guiding the user through the questions and providing explanations for both the questions and the answers. As a result, the user gets educated on risks and threats to ensure the ethical aspect of accountability.

The output is a report that includes: the data protection risk profile, an advice on whether to proceed or not, and suggested mitigations. The risk profile contains 1) a set of potential data protection issues and corresponding scores (according to DPIA questionnaire answers); and 2) a list of risks associated to the adoption of a given cloud service grouped into 3 categories: service, security and privacy (see Table 6) – if the user has selected a CSP.

The tool also logs the offered advice and the user's decision for accountability purposes.

The next subsections explain the development of the tool by first introducing its interface and data flow, and then discussing its components, architecture and implementation details. In addition, we used the tool to perform the data protection risk assessment of a use-case (see Section 6).

5.1 Tool Interface and Data Flow

DPIAT is a web-based tool for individual working in SMEs. The independent web interface enables easy and user friendly access and experience. The landing page asks the user whether they would like to start with an **easy-mode** questionnaire to see if they need to answer the full **expert-mode** questionnaire. The **easy-mode** questionnaire consists of preliminary screening questions (6 questions) to make a quick assessment of the transaction being carried by the user. Certain answers from the user will lead the tool to direct him to the expert-mode questionnaire to carry on with a full data protection risk assessment i.e. if the project contains sensitive data to be stored in the cloud. The **expert-mode** questionnaire is the one described in section 3 and contains a set of 56 questions.

ection Impact Assessment Tool

Please choose a Questionnaire:

This tool is a decision support tool to help you identify the risks involved in a transaction such as buying or using new cloud service/service provider. The tool is built on a risk and trust model to perform a thorough risk assessment to your configuration and environment. It will also help you understand the risks by providing information about their meanings and consequences. If you don't know already, use the 'Easy Mode Screening' to see whether you need the extended risk assessment mode.

Select a service provider

Cat 

Pre-Screening Questions

The privacy quick scan mode indicates whether an extended Data Protection Impact Assessment would be necessary or recommended. It includes a set of 6 questions, which assesses if the information you deal with constitute personal data or not, and then it evaluates the kind of information processed, its sensitivity, the purposes of the processing, the actors involved and the extent with which the information is likely to be diffused.

For a consistent and accurate result regarding the risks of particular processing operations, the completion of both questionnaires is necessitated: the Easy Mode Screening is but a pre-screening apt to tell you whether you would need to undertake the extended Privacy Impact Assessment or not.

[take this questionnaire](#)

Screening Questions

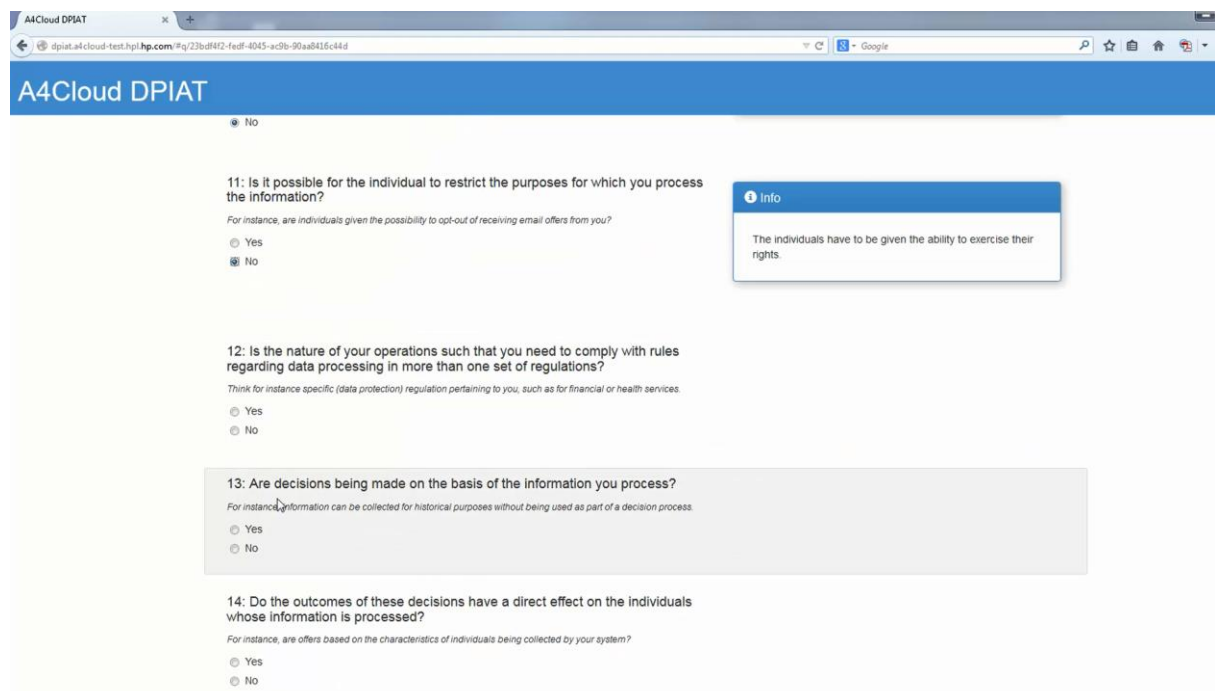
The extended Privacy Impact Assessment includes 56 questions. The questions are grouped into five topical areas, which refer to: 1) the type of project, 2) the collection and use of data, 3) the project's storage and security policies, 4) transfer of info, and 5) cloud specific issues.

The aim of this set of questions is to assess in a granular manner how the interactions between you and the CSP you deal with impact your users' rights to privacy and data protection, and how your system is designed – if so – to prevent or mitigate the potential adverse outcomes of those interactions.

You are to answer all questions to the best of your knowledge, if necessary asking the relevant professionals in your undertaking before answering; some questions, though, allow you to answer "I do not know" (yet!), but please do mind – you are supposed to know.

[take this questionnaire](#)

Figure 3 DPIAT initial screen



The screenshot shows the A4Cloud DPIAT web application in a browser. The page title is "A4Cloud DPIAT". The main content area displays a questionnaire with the following questions:

- 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?
☐ Yes
☒ No
- 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.
☐ Yes
☐ No
- 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.
☐ Yes
☐ No
- 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?
☐ Yes
☐ No

A tooltip is displayed on the right side of the screen, containing the following information:

Info

The individuals have to be given the ability to exercise their rights.

Figure 4 DPIAT tooltip displaying information about the selected options

5.2 Tool Components and Architecture

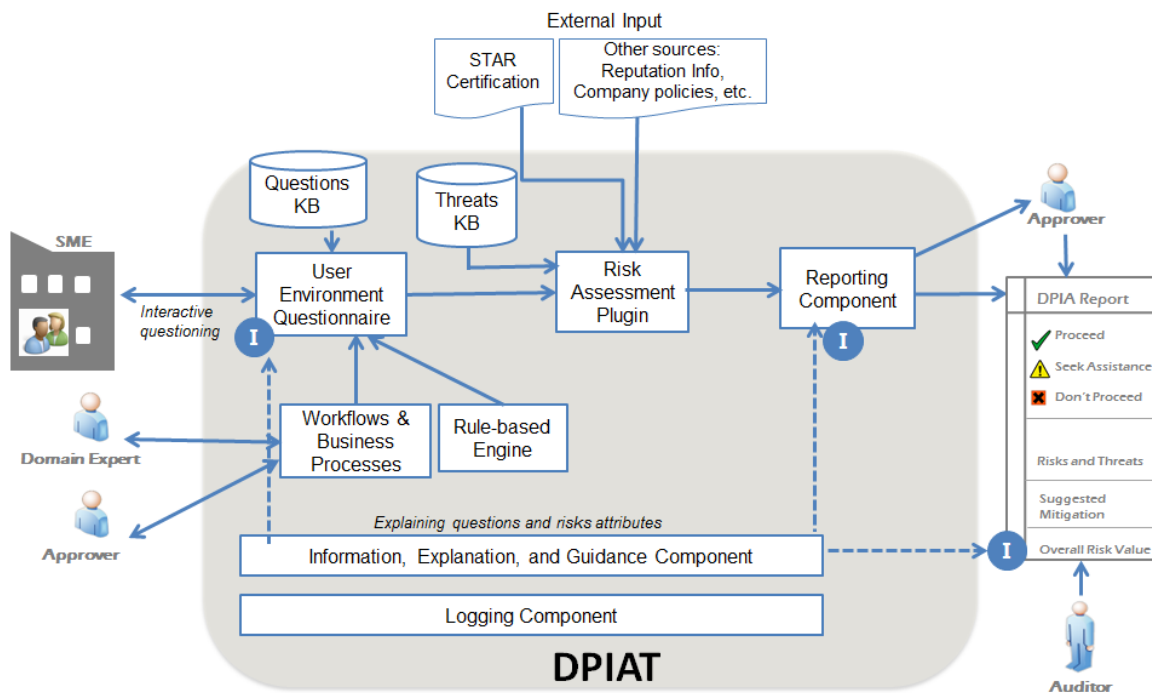


Figure 5 DPIAT Components

The tool consists of several components shown in Figure 5 DPIAT Components. These components are:

User Environment Questionnaire- Based on a pre-defined set of questions discussed in Section 3 and extracted from the questions knowledgebase, the tool asks the user -in the form of successive questions- for information about the project involved in the intended transaction (or the type of data that are going to be used in the transaction). The questionnaire is dynamic; some answers trigger additional questions. The rules to which questions will be shown depending on the answers are handled by the rule-based engine.

In addition, the tool asks the user to optionally select a CSP from a list of around 50 providers, which answered to the CAIQ.

Rule-based Engine- Certain answers to the screening questionnaire can lead to extra questions. Therefore, the rule-based engine sets up and processes the rules according to the path taken when the user answers with specific answers i.e. If answer is *no*, jump two questions ahead because the next two questions are no longer relevant/applicable.

Risk Assessment Plugin- After gathering the answers of the user, the User Environment Component passes a list of these answers to the plugin which in return assesses the risks based on the model discussed in Section 4 and then passes the assessment to the reporting component.

Reporting Component- This component is responsible for presenting the user with a complete assessment report in a comprehensible and user-friendly format. It pulls explanation and information from the information and guidance component to educate the user on the featured results. In addition, the tool allows the user to compare the risk profiles of any two providers, thus helping to select the most suitable CSP from the security point.

Information and explanation Component- For each question asked to the user, a helping text is provided to explain not only the meaning of the question but also the implications of the answers. This

component feeds the explanation-text to the interface to help a user in understanding the questions and the risks.

Logging Component- For the purpose of accountability and to make certain that the user was informed of the possible risks to a certain transaction; this component logs the values of the answers to the questionnaire and the final report given to him.

5.3 Tool Implementation

Figure 6 shows details about the DPIAT implementation. The tool is a web-based tool connecting to a database of predefined questions and available responses regarding the user's requirements for a given project. The server-side application and web-service (Questionnaire Provider) is written in Java. This application provides access to the questionnaire data and also provides a rules-engine that helps determine the flow of the questionnaire for the client as well as providing further details and information based on the user's responses to the questions offered. The rules engine is based on the Drools¹²⁸ library (Rules management solution which provides a rule engine).

The client side application is implemented using HTML5 and JavaScript and utilises a number of open-source libraries to simplify the underlying business logic layer. These libraries include Backbone and Marionette¹²⁹ (which enable a simple MVC structure in the client UI), jQuery¹³⁰, Underscore¹³¹ and Bootstrap¹³² to simplify the styling of the application.

In addition, a questionnaire administration application has also been introduced. This component allows authorised users to create and edit questionnaires and their associated Questions/Answers as needed.

¹²⁸ Drools: www.drools.org

¹²⁹ Marionette: <http://marionettejs.com/>

¹³⁰ jQuery: <http://jquery.com/>

¹³¹ Underscore: <http://underscorejs.org/>

¹³² Bootstrap: <http://getbootstrap.com/>

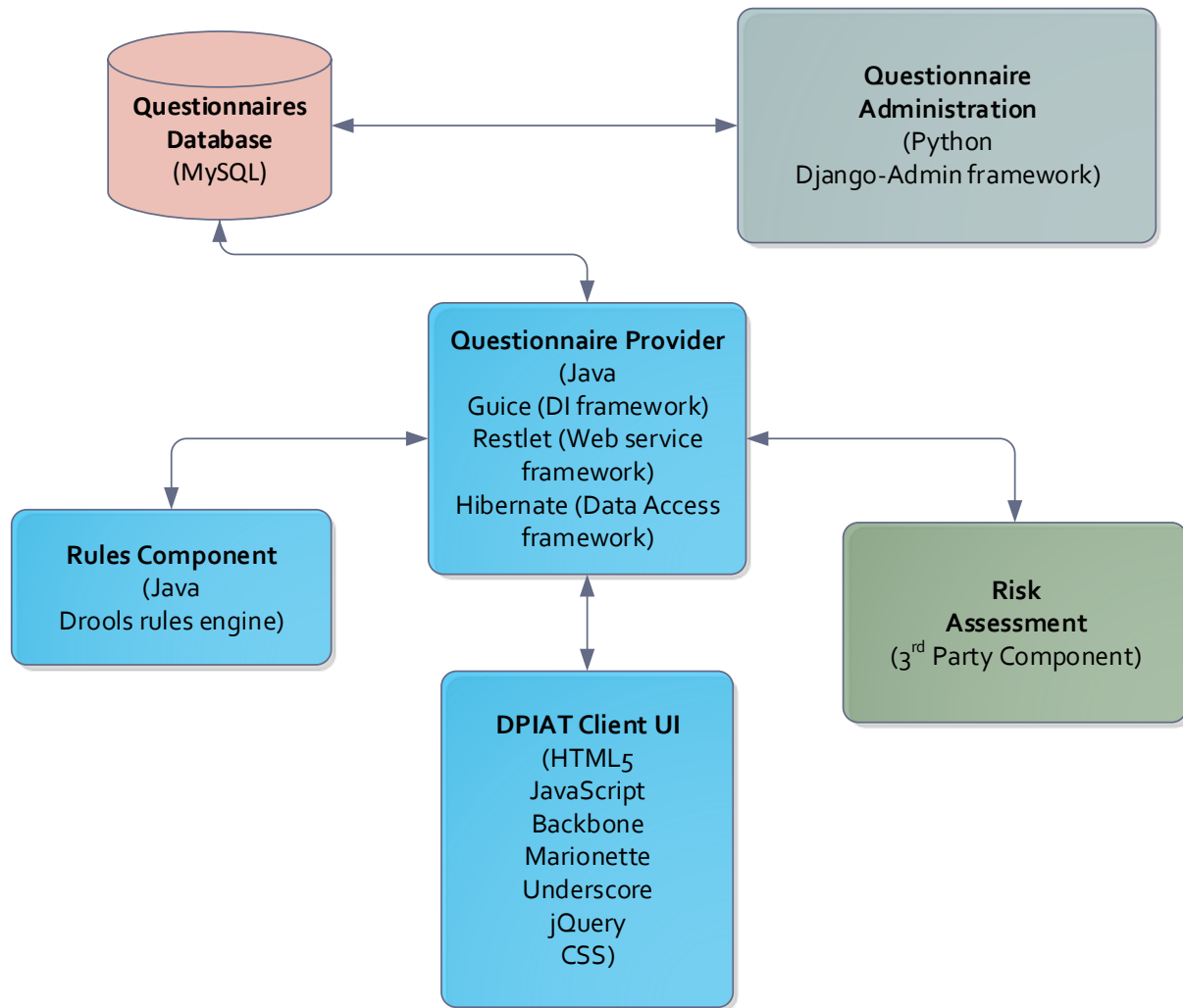


Figure 6 Technologies used in the DPIAT implementation

The goal of the Risk Assessment Plugin is to compute the risk indicators for the configuration informed by the user via the User Environment Questionnaire component. The plugin interacts with the other components via a RESTful API in JSON format.

The plugin uses two data sources for computing risk scores:

- The threats knowledge base: containing 35 risks (see Table 6), 58 related vulnerabilities (see Table 7) for cloud systems, and the relations between risks, vulnerabilities and mitigating controls;
- External input: we use information from CSA STAR on how CSPs implement their security controls (see Section 4).

Other data sources, such as company policies (see D34.1 and D34.2) and reputation information may be considered in the future versions of the tool.

6 Use case analysis

We present initially the Cloud Risk Assessment of the A4Cloud Business Use Case 2, defined in the B-3 use case development work package (Bernsmed et al, 2013), where an SME extends its ERP functionality with a SaaS to m its relationship with its customers. We follow the approach introduced in Section 4.2. Then we show how these results are incorporated in the overall data protection impact assessment.

6.1 Cloud adoption risk assessment

The SaaS ERP offering is used by a large supermarket chain operating in southern France. Among other business functionality, it is also used to support the loyalty program that its customers can join to benefit from special product offers and discounts. The service offered by the supermarket tracks customer behaviour in order to determine their shopping habits and provide more personalized offers, that customers are more likely to benefit from, respecting at the same time the customers' privacy. The SaaS is itself built upon other cloud services, notably a PaaS and an IaaS solution offered by third parties depicted in Figure 6.

The involved parties are MarchéAzur (the supermarket chain, the cloud consumer and at the same time data controller), Check-It-Out, the SaaS provider; PaaSPort (PaaS provider); and InfraRed (IaaS provider) are all operating their cloud offerings, at the software, platform and infrastructure level respectively. In addition, Check-it-out (ISV) is offering platform extension in form of the SaaS offering that can be utilized by other cloud services. We conduct the the assessment from the point of view of MarchéAzur, as the data controller, to illustrate our approach.

MarchéAzur operates both a mobile application that is targeted at their customers to collect shopping information, as well as the back-office CRM (Customer Relationship Management) service operated by its business analysts. Data utilized by these applications is coming from the on-premise ERP system still operated by MarchéAzur. It is mainly information about the products offered in supermarket stores, information related to marketing campaigns and possible discount offers and other business data consumed by the analytics service.

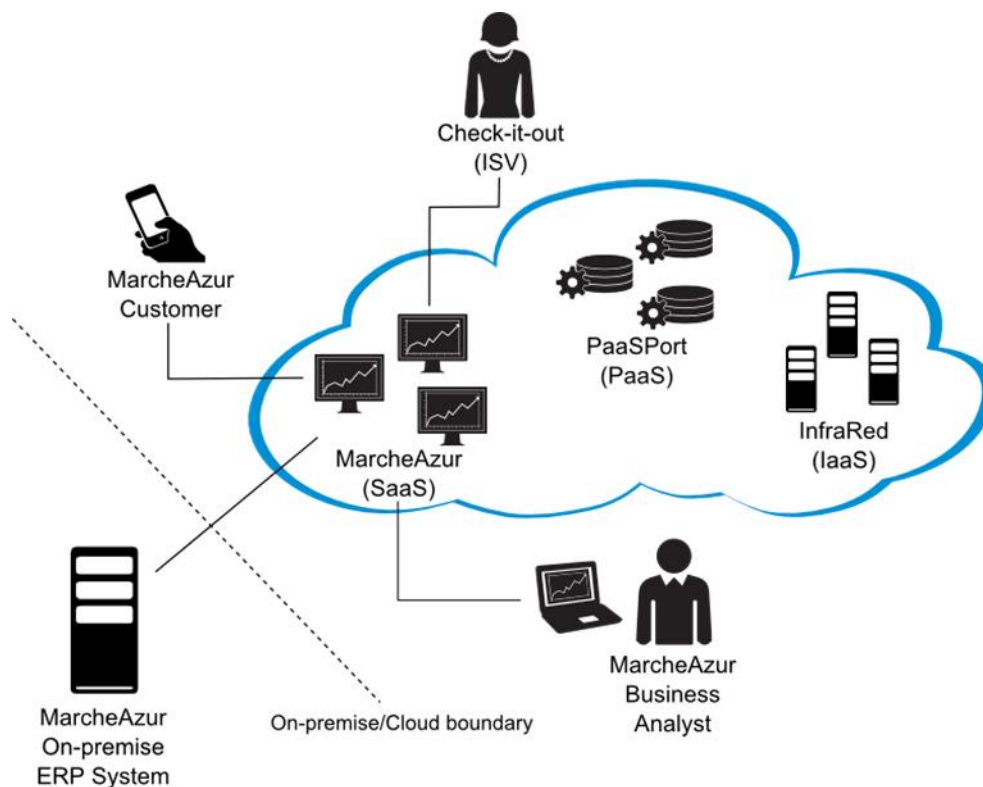


Figure 7 Conceptual overview of the cloud-based ERP business use case

In order to gather control implementation data, we generated a profile for the Check-it-Out SaaS provider by combining typical answers we collected from the CSA Star registry and collected from multiple SaaS providers present there (for more details on the data collection see Section 4.2). Its corresponding profile for the 198 questions of the CAIQ is given in Table 13 in the Appendix.

Consider R-23, data protection risks. According to ENISA, it is related to the following vulnerabilities:

- V29 - Storage of data in multiple jurisdictions and lack of transparency about this
- V30 - Lack of information on jurisdictions

We mapped the following control groups from the CCM as the more directly mitigate these specific vulnerabilities:

•	DG	01	Data Governance	Ownership / Stewardship
•	DG	02	Data Governance	Classification ¹³³
•	LG	02	Legal	Third Party Agreements
•	DG	03	Data Governance	Handling / Labeling / Security Policy
•	DG	04	Data Governance	Retention Policy
•	CO	05	Compliance	Information System Regulatory Mapping
•	IS	03	Information Security	Policy
•	IS	04	Information Security	Baseline Requirements
•	IS	05	Information Security	Policy Reviews
•	IS	06	Information Security	Policy Enforcement
•	IS	22	Information Security	Incident Management
•	IS	23	Information Security	Incident Reporting
•	IS	24	Information Security	Incident Response Legal Preparation
•	IS	26	Information Security	Acceptable Use
•	LG	01	Legal	Non- Disclosure Agreements
•	LG	02	Legal	Third Party Agreements
•	SA	01	Security Architecture	Customer Access Requirements
•	RI	02	Risk Management	Assessments
•	RI	03	Risk Management	Mitigation / Acceptance
•	RI	04	Risk Management	Business / Policy Change Impacts
•	RI	05	Risk Management	Third Party Access

We need to compute the vulnerability parameter, ε_k , of the SaaS offer for each of the $K = 1..53$ different vulnerabilities. As an example we compute the values for ε_{29} and ε_{30} using equation (5) from Section 4.4:

$$\varepsilon_{29} = \frac{\sum_{m=1}^n r_{m,29} \times q_m}{\sum_{m=1}^n r_{m,29}} = 0.44444444 \quad (V29)$$

$$\varepsilon_{30} = \frac{\sum_{m=1}^n r_{m,30} \times q_m}{\sum_{m=1}^n r_{m,30}} = 0.44444444 \quad (V30)$$

Where m ranges from 1 until n , the number of controls mapped to that particular vulnerability, from V26 and V30 exactly the same control groups are mapped to these vulnerabilities there are $n = 18$ different controls. According to the Table 9 in the Appendix, there are eight controls implemented by the provider among the control groups listed above. This explains why the computed values for ε_{29} and ε_{30} are the equal. The values for the further vulnerability parameters for this use case can be found in Table 11.

Next, we compute the vulnerability index of the risk R-23 for this CSP as follows using the values of the vulnerability parameter for the data protection risk, as defined by the ENISA. The result for ϑ_{23} is

¹³³ This control group contains questions related to physical location of virtual resources in the cloud.

the same as for ε_{29} and ε_{30} , since their sum divided by the total number of vulnerabilities for R-23 is two.

$$\vartheta_{23} = \frac{\sum_{k=1}^{53} v_{ki} \times \varepsilon_k}{\sum_{k=1}^{53} v_{ki}} = 0.44444444$$

The calculation of the probabilities must proceed in this way for all 35 different risks. The screenshot in Figure 8 presents the output of the DPIA tool plugin¹³⁴, developed by SAP, with the values for the vulnerability index for all the risks concerning this fictitious service from “Check-it-Out”. The complete vulnerability indices for this CSP are given in Table 12.

For the impact parameter α_i we considered the profile of a cloud service consumer processing personal data in the cloud, thus associating the following values to γ_k , as indicated in Equation (4):

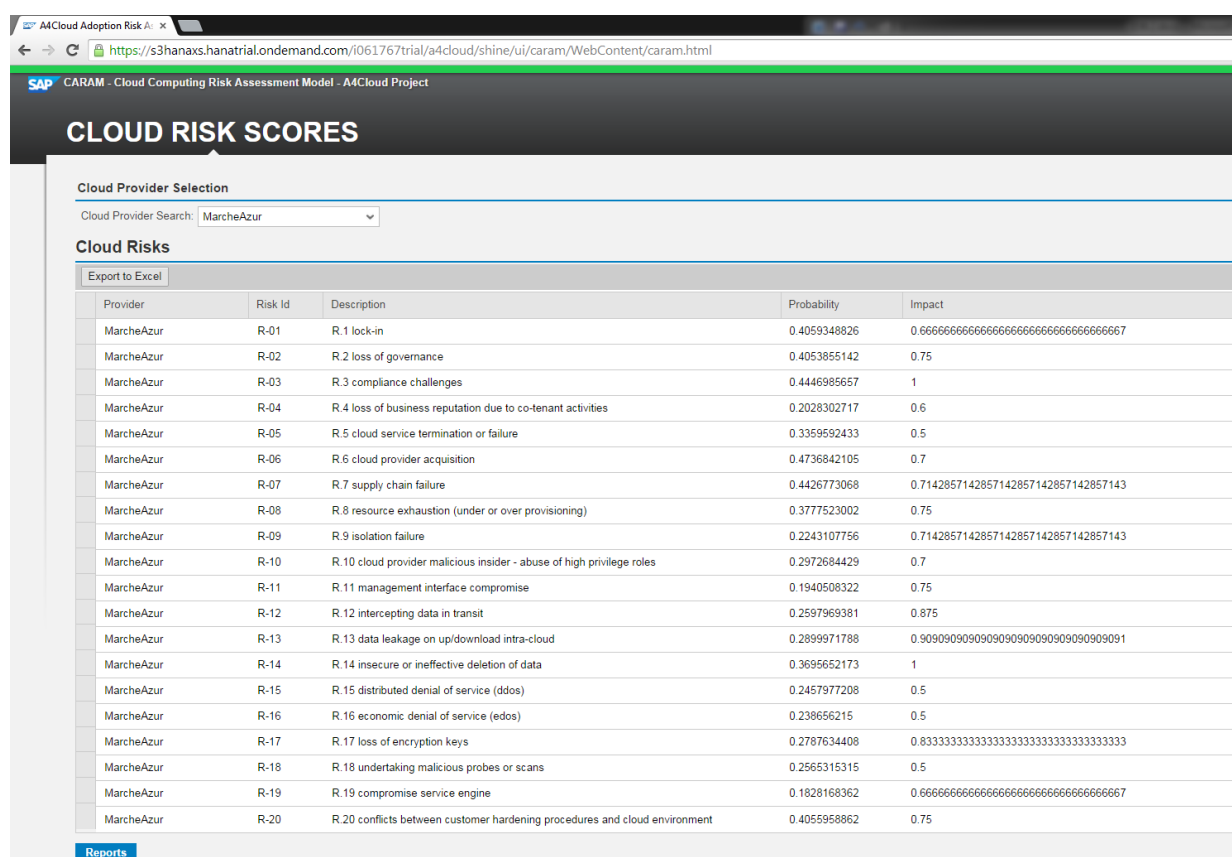
Table 4 Relevant assets for the Use Case

AssetId	Description	$\gamma_{k^{135}}$
A-01	A1. Company reputation	1
A-02	A2. Customer trust	1
A-03	A3. Employee loyalty and experience	1
A-04	A4. Intellectual property	0
A-05	A5. Personal sensitive data	1
A-06	A6. Personal data	1
A-07	A7. Personal data: critical	1
A-08	A8. HR data	1
A-09	A9. Service delivery: real time services	0
A-16	A16. Network (connections etc.)	0
A-11	A11. Access control / authentication / authorization	1
A-12	A12. Credentials	1
A-13	A13. User directory (data)	1
A-14	A14. Cloud service management interface	1
A-15	A15. Management interface APIs	1
A-17	A17. Physical hardware	0
A-18	A18. Physical buildings	0
A-19	A19. Cloud Provider Application (source code)	0
A-10	A10. Service delivery	0
A-20	A20. Certification	1
A-21	A21. Operational logs (customer and cloud provider)	1
A-22	A22. Security logs	1
A-23	A23. Backup or archive data	1

¹³⁴ Accessible under

<https://s3hanaxs.hanatrial.ondemand.com/i061767trial/a4cloud/shine/ui/caram/WebContent/caram.html> in order to access the application, it is necessary to create an account at <https://account.hanatrial.com> and request access to a4cloud@a4cloud.eu.

¹³⁵ See equation (4).



The values for security and service risks were generated by our prototype, the Cloud Risk Assessment Plugin¹³⁶, given below according to Equations (6) through (8):

$$\begin{aligned}\beta_r &= 0.32379407696 \\ \beta_s &= 0.25398002829 \\ \beta_e &= 0.26281600905\end{aligned}$$

The values show that for privacy, security and service the selected provider would be classified as low, considering the qualitative ranges explained in Section 4. The computation of the relative impact for the three categories follows a very similar approach. The cloud consumer profile must contain the evaluation for each of the 23 different assets suggested by ENISA, given in Table 8. This can be captured by the DPIAT interface.

6.2 Data protection impact assessment

Concerning the BUC2, the pre-screening phase of the DPIA would be answered as follows:

Question 1	Based on the information that you process, can you identify one or more individuals about whom you are processing information?
Answer	Yes. MarcheAzur associates a fidelity identifier to further personal data of its customers.
Question 2	Does the information that you process reveal certain characteristics of individuals?
Answer	Yes. It is possible to build customer profiles revealing their shopping habits and to infer further data, such as average income and family situation.
Question 3	Do you deal with any kind of the following categories of information?
Answer	Selects "location data" and "Credit Card Data"
Question 4	What is the scale of your processing operations?
Answer	Large. More than 10 thousand individuals.
Question 5	Is the nature, scope and/or purpose of your business, profession or activity based on a regular and systematic monitoring either of any natural person(s) or of publicly accessible areas?
Answer	No.
Question 6	How likely is that incidents will raise concerns amongst individuals and/or legal entities?
Answer	Small (3).
Question 7	Are there any third parties involved in the storage, processing, use, or transfer of any information that you deal with?
Answer	Yes. MarcheAzur uses cloud services; therefore further data processors are involved.

As a result, the DPIA pre-screening indicates that a full-fledged DPIA needs to be conducted for the project. We selected a few questions for discussion here. The complete assessment of the use case can be seen in Appendix 9.3.

The questionnaire allows for dynamic interactions with the user of the DPIAT. For example, question 18 "Does your project involve the use of existing personal information for new purposes?" is responded by MarcheAzur by "No". This makes unnecessary to address the questions from 19 to 22 who allow gathering more detailed information on the processing of existing data for new purposes.

While answering the questionnaire for BUC 2 we considered the usage of the A4Cloud toolkit for multiple situations. For instance, the Question 24: "Are procedures in place to provide individuals access to information about themselves?" received the answer "Yes" because we envisage

¹³⁶ The corresponding web service can be accessed under https://s3hanaxs.hanatrial.ondemand.com/i061767trial/a4cloud/shine/services/relativeRisks.xsodata/RELATIVE_RISKS/

demonstrating data subject access via the Data Track tool (for more information refer to deliverable D45.1).

The Question 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?” requires a lot of attention from the respondent, in particular in a cloud context. The question presents a list of more than 20 items ranging from access control, segregation of duty, to anonymisation, pseudonymization and sticky policies. Collecting this information from data processors in the chain can be difficult and time consuming. Also, it may not be straightforward for the cloud customer to obtain this information from the cloud provider, depending on how transparent the provider is.

Another relevant example to comment is the Question 30: “Do you have a Data Security Policy?” in BUC2, MarcheAzur has set up an accountability policy to express all its obligations as data controller about the personal data handling processes it carries out. Furthermore, it also has policies concerning the allowed data transfers indicating how further processors in the chain; in this case its infrastructure provider should handle virtual resources in the cloud. The policy also determines access and usage control rules in the APPL syntax – for more details, see deliverables D23.2 and D34.2.

It is worth mentioning that the current A4Cloud prototypes on D3 – accountability and compliance enforcement tools have the capability to detect incidents about potentially non-compliant data transfers in the cloud and also to notify data controllers and subjects about them, according to what is expressed in the accountability policy governing the personal data handling. That is why for BUC2 we answered “Yes” to Question 38: “Do you take action in order to notify individuals in case of (security) incidents?” There are ongoing discussions and developments on the work package D4 – contracts, SLAs and Remediation on incident response procedures, which may involve additional incident types.

After filling in the screening questions for the BUC2, we can estimate the probability and impact of non-compliance respectively as 45 and 40 according to the impact we have provided for each answer. These values fall in the “Low” risk range. The value is the sum of the weights assigned to each answer selected by the respondent. The tool calculates the maximum score in the Impact parameter and the Likelihood parameter that a user could theoretically achieve, and divide that score into five intervals, and then assign to each interval a number from 0 to 4 (very low, low, medium, high, very high), which added to the score of the other parameter after the same operation would give us the overall risk level of the processing activities of the user.

The range of possible maximum values was split in five categories from very low to very high risk. There is ongoing work to adjust the value ranges and to consider the cloud risk assessment scores in order to produce the DPIA report to the user.

This exercise allowed us to obtain some insight on how complex is the task of running the DPIA screening. Ideally the DPIA should be conducted with the organisation's Data Protection Officer, the Security Information Officer and the Project Manager for the project under analysis as to dispose of all necessary information at the time of the assessment. The questionnaire contains enough information, exposed in an understandable way, such that non specialised personnel can perform an assessment and understand the results.

7 Conclusions

The deliverable reports the results obtained in the second and final year of the work package C6. The initial objectives were achieved, namely, the creation of a risk and trust model adapted to the cloud, a risk assessment methodology that encompasses cloud specific and further risks in the cloud that fits existing standards and practices. We also proposed a revised Data Protection Assessment methodology, supported by a tool, helping users to understand, assess, and to select cloud providers that offer acceptable standards in terms of privacy, security and service risks. Performing the analysis of the business use case allowed for the adjustment of multiple parameters, and the simplification of the usage of the tool, allowing us to focus on the most relevant aspects of the data protection and risk impact assessments.

Although the work package is concluded there are several improvements that will be carried out in the methodology and in the prototype, because there is considerable interest by the involved partners. User assessments will very likely, be conducted by the partners involved in this work, to provide new directions and priorities for the next versions of the prototype for DPIAT.

8 References

- Article 29 Data Protection Working Party (2014). Statement on the role of a risk-based approach in data protection legal frameworks (WP218), May. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.
- Bennett, C.J. and Raab, C.D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. MIT Press, Cambridge, Massachusetts
- Bernsmed, K., Felici, M., Santana De Oliveira, A., Sendor, J., Brede Moe, N., Rübsamen, T., ... Hasnain, B. (2013). Use Case Descriptions (Deliverable No. D:B-3.1) (p. 68). A4Cloud.
- CambridgeSoft (2010) ChemBioOffice Cloud – An Integrated Decision Support System for CHDI. <http://chembionews.cambridgesoft.com/WhitePapers/Default.aspx?whitePaperID=43>
- Cayirci, E. and Oliveira, A.S. (2013), “Modelling Risk and Trust for Cloud Service Mashups”, IEEE Transactions on Computers (submitted).
- Cayirci, E. Garaga A. Oliveira, A.S. Roudier, Y. (2014), Cloud Adoption Risk Assessment Model”, 2014 International Workshop on Advances in Cloud Computing Legislation, Accountability, Security and Privacy (CLASP) (accepted).
- Centre for Information Policy Leadership (CIPL) (2014). A Risk-based Approach to Privacy: Improving Effectiveness in Practice. http://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf
- CNIL (2012). Recommendations for Companies Planning to Use Cloud Computing Services. http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf
- CNIL (2012). Methodology for Privacy Risk Management, June 2012.
- Cloud Security Alliance (CSA) (2011) Security guidance for critical areas of focus in cloud computing, v3.0. <http://www.cloudsecurityalliance.org/guidance/>
- CSA (2013). The notorious nine: Cloud computing top threats in 2013, v.1.0. <http://cloudsecurityalliance.org/research/top-threats/>
- ENISA (2009). Cloud Computing - Benefits, risks and recommendations for information security.
- Felici, M. and Pearson, S. (2014). Accountability, Risk, and Trust in Cloud Services: Towards an Accountability-Based Approach to Risk and Trust Governance. Proc. SERVICES, IEEE, pp. 105-112.
- Habib, S. (2013). A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces. CCSW, 459–468. doi:10.1109/TrustCom.2013.58
- Harbird, R., Ahmed, M., Finkelstein, A., McKinney, E., Burroughs, A. (2007). Privacy Impact Assessment with PRAIS. <http://www.cs.ucl.ac.uk/staff/A.Finkelstein/papers/hotpets.pdf>
- Hall, M. *et al* (2009). *The WEKA Data Mining Software: An Update*; SIGKDD Explorations, Volume 11, Issue
- Information Commissioners Office (ICO) (2009). Privacy Impact Assessment Handbook. <http://www.ico.gov.uk/handbook/June.2009>
- ICO (2012) Guidance for Companies on the Use of Cloud Computing, v1.1 http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing
- Ninja Marnau (2010). *D1.2.4 Cloud Computing – Data Protection Impact Assessment*, Deliverable, TClouds project.
- NIST (2011). Guidelines on Security and Privacy in Public Cloud Computing, SP 800-144. <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>
- OECD (2013). Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data <http://www.oecd.org/sti/economy/2013-oecd-privacy-guidelines.pdf>
- Office of the Privacy Commissioner of Canada (2011). Securing Personal Information: A Self-Assessment Tool for Organisations. <http://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1>

- Office of the Privacy Commissioner of Canada (OPCD) (2011). Privacy Impact Assessments. http://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp
- De Oliveira A.S, Garaga A., Martucci L. A. , Felici M., Alnemr R., Stefanatou D. , Niezen M., Fernandez C., Nuñez D., Hasnain B. , Vranaki A. and Cayirci E. D:C-6.1: Risk and trust models for accountability in the cloud. Deliverable. A4Cloud project, 2013.
- Pearson, S. (2010). Simple Mode: Addressing Knowledge Engineering Complexity in a Privacy Expert System, HP Labs External Technical Report, HPL-2010-75, June. Available via <http://www.hpl.hp.com/techreports/2010/HPL-2010-75.html>
- Pearson, S. and Sander, T. (2012). A Decision Support System for Privacy Compliance. In: Threats, Countermeasures, and Advances in Applied Information Security, Manish Gupta, John Walp, and Raj Sharman (eds.), Information Science Reference, IGI Global, New York, pp. 158-180.
- Pearson, S., et al. (2009). Scalable, Accountable Privacy Management for Large Organizations, INSPEC 2009: 2nd International Workshop on Security and Privacy Distributed Computing, Enterprise Distributed Object Conference Workshops (EDOCW 2009), IEEE, pp. 168-175.
- Sander, T. and Pearson, S. (2010). Decision Support for Selection of Cloud Service Providers. International Journal on Computing (JoC), GTSF, vol.1, no. 1, pp. 106-113, August.
- Tancock, D. *et al* (2010). *The Emergence of Privacy Impact Assessments*. Tech Report HPL-2010-63.
- Tancock, D., Pearson, S. and Charlesworth, A. (2010). Analysis of Privacy Impact Assessments within Major Jurisdictions. Proc. PST 2010, Ottawa, Canada, IEEE, pp. 118-125.
- Tancock, D., Pearson, S. and Charlesworth, A. (2013). A Privacy Impact Assessment Tool for Cloud Computing. Privacy and Security for Cloud Computing, S. Pearson and G. Yee (eds.), Computer Communications and Networks, Springer, pp. 73-123.
- United States Department of Homeland Security (2007) Privacy Threshold Analysis (PTA). http://www.dhs.gov/xlibrary/assets/privacy/DHS_PTA_Template.pdf

9 Appendices

9.1 Cloud security risk assessment input

Table 6 ENISA's list of risk scenarios and their categories

Risk Category	Risk name
Policy & Organizational	P1.Lock-in P2.Loss of governance P3.Compliance challenges P4.Loss of business reputation due to co-tenant activities P5.Cloud service termination or failure P6.Cloud provider acquisition P7.Supply chain failure
Technical	T1. Resource exhaustion (under or over provisioning) T2. Isolation failure T3. Cloud provider malicious insider - abuse of high privilege roles T4. Management interface compromise (manipulation, availability of infrastructure) T5. Intercepting data in transit T6. Data leakage on up/download, intra-cloud T7. Insecure or ineffective deletion of data T8. Distributed denial of service (DDoS) T9. Economic denial of service (EDOS) T10. Loss of encryption keys T11. Undertaking malicious probes or scans T12. Compromise service engine T13. Conflicts between customer hardening procedures and cloud environment
Legal	L1. Subpoena and e-discovery L2. Risk from changes of jurisdiction L3. Data protection risks L4. Licensing risks
Not Specific to the Cloud	N1. Network breaks N2. Network management (i.e., network congestion / disconnection / non-optimal use) N3. Modifying network traffic N4. Privilege escalation N5. Social engineering attacks (i.e., impersonation) N6. Loss or compromise of operational logs N7. Loss or compromise of security logs (manipulation of forensic investigation) N8. Backups lost, stolen N9. Unauthorized access to premises (including physical access to machines and other facilities) N10. Theft of computer equipment N11. Natural disasters

Table 7 ENISA's list of vulnerabilities

Cloud Specific Vulnerabilities

- V1. Authentication Authorization Accounting (AAA) vulnerabilities
- V2. User provisioning vulnerabilities
- V3. User de-provisioning vulnerabilities
- V4. Remote access to management interface
- V5. Hypervisor vulnerabilities
- V6. Lack of resource isolation
- V7. Lack of reputational isolation
- V8. Communication encryption vulnerabilities
- V9. Lack of or weak encryption of archives and data in transit
- V10. Impossibility of processing data in encrypted form
- V11. Poor key management procedures
- V12. Key generation: low entropy for random number generation
- V13. Lack of standard technologies and solutions
- V14. No source escrow agreement
- V15. Inaccurate modelling of resource

- V16. No control on vulnerability assessment process
- V17. Possibility that internal (cloud) network probing will occur
- V18. Possibility that co-residence checks will be performed
- V19. Lack of forensic readiness
- V20. Sensitive media sanitization
- V21. Synchronizing responsibilities or contractual obligations external to cloud
- V22. Cross-cloud applications creating hidden dependency
- V23. SLA clauses with conflicting promises to different stakeholders
- V24. SLA clauses containing excessive business risk
- V25. Audit or certification not available to customers
- V26. Certification schemes not adapted to cloud infrastructures
- V27. Inadequate resource provisioning and investments in infrastructure
- V28. No policies for resource capping
- V29. Storage of data in multiple jurisdictions and lack of transparency about this
- V30. Lack of information on jurisdictions
- V31. Lack of completeness and transparency in terms of use

Vulnerabilities not Specific to the Cloud

- V32. Lack of security awareness
- V33. Lack of vetting processes
- V34. Unclear roles and responsibilities
- V35. Poor enforcement of role definitions
- V36. Need-to-know principle not applied
- V37. Inadequate physical security procedures
- V38. Misconfiguration
- V39. System or OS vulnerabilities
- V40. Untrusted software
- V41. Lack of, or a poor and untested, business continuity and disaster recovery plan
- V42. Lack of, or incomplete or inaccurate, asset inventory
- V43. Lack of, or poor or inadequate, asset classification
- V44. Unclear asset ownership
- V45. Poor identification of project requirements
- V46. Poor provider selection
- V47. Lack of supplier redundancy
- V48. Application vulnerabilities or poor patch management
- V49. Resource consumption vulnerabilities
- V50. Breach of nda by provider
- V51. Liability from data loss (cp)
- V52. Lack of policy or poor procedures for logs collection and retention
- V53. Inadequate or misconfigured filtering resources

Table 8 ENISA's list of assets

Assets

- A1. Company reputation
- A2. Customer trust
- A3. Employee loyalty and experience
- A4. Intellectual property
- A5. Personal sensitive data
- A6. Personal data
- A7. Personal data - critical
- A8. HR data
- A9. Service delivery – real time services
- A10. Service delivery
- A11. Access control / authentication / authorization (root/admin v others)
- A12. Credentials
- A13. User directory (data)
- A14. Cloud service management interface
- A15. Management interface APIs
- A16. Network (connections, etc.)
- A17. Physical hardware
- A18. Physical buildings
- A19. Cloud Provider Application (source code)
- A20. Certification
- A21. Operational logs (customer and cloud provider)
- A22. Security logs

A23. Backup or archive data

Table 9 Mapping CAIQ questions to vulnerabilities

Control Group	Vulnerabilities mitigated
Audit Planning CO-01	V02, V03, V13, V14, V16, V23, V25, V26, V27, V29, V33, V35, V50,
Independent Audits CO-02	V02, V03, V13, V14, V16, V23, V25, V26, V27, V29, V33, V35, V50,
Third Party Audits CO-03	V02, V03, V13, V14, V16, V23, V25, V26, V27, V29, V33, V35, V50,
Contact / Authority Maintenance CO-04	V14, V21, V29, V30,
Information System Regulatory Mapping CO-05	V07, V08, V09, V10
Intellectual Property CO-06	V34, V31, V35, V44
Intellectual Property CO-07	V34, V31, V35, V44
Intellectual Property CO-08	V34, V31, V35, V44
Ownership / Stewardship DG-01	V22, V23, V24, V29, V30, V31, V33, V34, V35, V42, V43, V44
Classification DG-02	V32, V36, V37,
Handling / Labelling / Security Policy DG-03	V01, V04, V05, V06, V08, V10, V11, V12, V19, V20, V22, V32, V37, V39,
Retention Policy DG-04	V21, V29, V44
Secure Disposal DG-05	V37, V42, V44, V51, V52
Nonproduction Data DG-06	V32, V36, V37, V43, V44,
Information Leakage DG-07	V1, V4, V5, V32, V36, V37
Risk Assessments DG-08	V16, V22, V29, V32, V33, V34, V44
Policy FS-01	V17, V32, V37,
User Access FS-02	V02, V03, V17, V19, V25, V29, V32, V37
Controlled Access Points FS-03	V17, V19, V32, V37
Secure Area Authorization FS-04	V22, V29
Unauthorized Persons Entry FS-05	V17, V19, V32, V37
Offsite Authorization FS-06	V22, V29
Offsite equipment FS-07	V6, V31, V42, V43, V44
Asset Management FS-08	V6, V31, V42, V43, V44
Background Screening HR-01	V17, V18, V50
Employment Agreements HR-02	V17, V18, V32, V34, V35, V50
Employment Termination HR-03	V17, V18, V50
Management Program IS-01	V1, V16, V32, V33, V34
Management Support / Involvement IS-02	V1, V32, V33, V34

Policy IS-03	V13, V19, V32, V33, V52
Baseline Requirements IS-04	V1, V5, V8, V9, V11, V12, V13, V17, V19, V32, V33, V39, V40
Policy Reviews IS-05	V03, V28, V32, V50, V52
Policy Enforcement IS-06	V32, V34, V35
User Access Policy IS-07	V1, V2, V3, V4, V6
User Access Restriction / Authorization IS-08	V6, V42, V43, V44
User Access Revocation IS-09	V3, V4, V17, V35
User Access Reviews IS-10	V1, V2, V3, V4, V17, V36
Training / Awareness IS-11	V32, V36
Industry Knowledge / Benchmarking IS-12	V5, V13, V32, V39, V40
Roles / Responsibilities IS-13	V34, V35
Management Oversight IS-14	V32, V34, V35
Segregation of Duties IS-15	V34, V36,
User Responsibility IS-16	V32, V34, V35
Workspace IS-17	V06, V40, V42, V43, V44
Encryption IS-18	V08, V09,
Encryption Key Management IS-19	V08, V09, V11, V12
Vulnerability / Patch Management IS-20	V02, V03, V05, V08, V16, V39, V40, V48
Antivirus / Malicious Software IS-21	V40, V48,
Incident Management IS-22	V34, V41, V52
Incident Reporting IS-23	V52
Incident Response Legal Preparation IS-24	V19, V30, V52
Incident Response Metrics IS-25	V52
Acceptable Use IS-26	V25, V31, V36, V43, V50
Asset Returns IS-27	V13, V31, V50
E-commerce Transactions IS-28	V08, V09, V10
Audit Tools Access IS-29	V05, V06, V39, V53
Diagnostic / Configuration Ports Access IS-30	V05, V06, V39, V53
Network / Infrastructure Services IS-31	V02, V15, V28, V31
Portable / Mobile Devices IS-32	V39, V48
Source Code Access Restriction IS-33	V48
Utility Programs Access	V04, V05, V39

IS-34	
Nondisclosure Agreements	V18, V23, V24, V25, V30, V31
LG-01	
Third Party Agreements	V21, V22, V23, V29
LG-02	
Policy	V28, V31, V34, V35, V52
OP-01	
Documentation	V15, V36, V38, V42, V43, V52, V53
OP-02	
Capacity / Resource Planning	V14, V15, V27, V28, V49, V50, V53
OP-03	
Equipment Maintenance	V5, V47
OP-04	
Program	V51
RI-01	
Assessments	V16, V24
RI-02	
Mitigation / Acceptance	V16, V24
RI-03	
Business / Policy Change Impacts	V16, V19, V24
RI-04	
Third Party Access	V21, V24, V41, V47, V52
RI-05	
New Development / Acquisition	V13, V40
RM-01	
Production Changes	V25, V36, V38, V50
RM-02	
Quality Testing	V15, V38, V40
RM-03	
Outsourced Development	V13, V40
RM-04	
Unauthorized Software Installations	V13, V40
RM-05	
Management Program	V41, V52
RS-01	
Impact Analysis	V16, V52
RS-02	
Business Continuity Planning	V23, V24, V25, V27, V28, V41, V47
RS-03	
Business Continuity Testing	V23, V24, V25, V27, V28, V41, V47
RS-04	
Environmental Risks	V37, V41
RS-05	
Equipment Location	V37, V41
RS-06	
Equipment Power Failures	V37, V41
RS-07	
Power / Telecommunications	V29, V45, V46
RS-08	
Customer Access Requirements	V21, V23, V45, V46
SA-01	
User ID Credentials	V1, V2
SA-02	
Data Security / Integrity	V13, V32
SA-03	
Application Security	V13, V48
SA-04	
Data Integrity	V08, V09
SA-05	
Production / Nonproduction Environments	V41, V45
SA-06	
Remote User Multifactor Authentication	V01
SA-07	
Network Security	V32

SA-08	
Segmentation	V06, V07, V53
SA-09	
Wireless Security	V32
SA-10	
Shared Networks	V32
SA-11	
Clock Synchronization	V39
SA-12	
Equipment Identification	V01
SA-13	
Audit Logging / Intrusion Detection	V01, V32
SA-14	
Mobile Code	V32

Table 10 Mapping ENISA risk scenarios to A4CLOUD risk categories

ENISA Risk Scenarios	Privacy	Security	Service
P1	0	0	1
P2	1	0	0
P3	1	1	1
P4	0	1	0
P5	0	0	1
P6	1	1	1
P7	0	0	1
T1	0	0	1
T2	1	1	0
T3	1	1	1
T4	1	1	1
T5	1	1	0
T6	1	1	0
T7	1	1	0
T8	0	0	1
T9	0	0	1
T10	1	1	0
T11	1	1	0
T12	1	1	1
T13	0	1	0
L1	1	1	0
L2	1	0	0
L3	1	1	0
L4	0	0	1
N1	0	0	1
N2	0	0	1
N3	0	0	1
N4	1	1	1
N5	0	1	0
N6	0	1	1
N7	0	1	1
N8	1	1	1
N9	1	1	0
N10	1	1	1
N11	0	0	1

Table 11 Vulnerability Parameter for BUC 2 SaaS

Vulnerability	Vulnerability Parameter
V01	0.149122807
V02	0.180851064
V03	0.180851064
V04	0.149122807

V05	0.184782609
V06	0.180851064
V07	0.242857143
V08	0.193181818
V09	0.22972973
V10	0.666666667
V11	0.283333333
V12	0.274193548
V13	0.386363636
V14	0.369565217
V15	0.369565217
V16	0.293103448
V17	0.22972973
V18	0.283333333
V19	0.375
V20	0.369565217
V21	0.444444444
V22	0.533333333
V23	0.45
V24	0.473684211
V25	0.347826087
V26	0.571428571
V27	0.470588235
V28	0.533333333
V29	0.444444444
V30	0.444444444
V31	0.473684211
V32	0.386363636
V33	0.386363636
V34	0.293103448
V35	0.290322581
V36	0.369565217
V37	0.173469388
V38	0.236111111
V39	0.217948718
V40	0.257575758
V41	0.244186047
V42	0.36
V43	0.3125
V44	0.333333333
V45	0.5
V46	0.470588235
V47	0.293103448
V48	0.217948718
V49	0.242857143

V50	0.5
V51	0.647058824
V52	0.34
V53	0.283333333

Table 12 Vulnerability Indices for the BUC2 SaaS

Risk	Vulnerability Index
R-01	0.405934883
R-02	0.405385514
R-03	0.444698566
R-04	0.202830272
R-05	0.335959243
R-06	0.473684211
R-07	0.442677307
R-08	0.3777523
R-09	0.224310776
R-10	0.297268443
R-11	0.194050832
R-12	0.259796938
R-13	0.289997179
R-14	0.369565217
R-15	0.245797721
R-16	0.238656215
R-17	0.278763441
R-18	0.256531532
R-19	0.182816836
R-20	0.405595886
R-21	0.356579984
R-22	0.444444444
R-23	0.444444444
R-24	0.473684211
R-25	0.219774235
R-26	0.219774235
R-27	0.211996849
R-28	0.235588738
R-29	0.222943394
R-30	0.240628942
R-31	0.240628942
R-32	0.171073581
R-33	0.173469388
R-34	0.173469388
R-35	0.244186047

Table 13 CAIQ answers for the MarcheAzur SaaS

Control Group	Control	Answer
CO-01	CO-01.1	Yes
CO-02	CO-02.1	Yes
CO-02	CO-02.2	Yes
CO-02	CO-02.3	Yes
CO-02	CO-02.4	Yes
CO-02	CO-02.5	Yes
CO-02	CO-02.6	Yes
CO-02	CO-02.7	Yes
CO-03	CO-03.1	Yes
CO-03	CO-03.2	Yes
CO-04	CO-04.1	Yes
CO-05	CO-05.1	Yes
CO-05	CO-05.2	Yes
CO-06	CO-06.1	Yes
CO-07	CO-07.1	NotAvailable
CO-08	CO-08.1	NotAvailable
DG-01	DG-01.1	Yes
DG-02	DG-02.1	Yes
DG-02	DG-02.2	Yes
DG-02	DG-02.3	Yes
DG-02	DG-02.4	Yes
DG-02	DG-02.5	Yes
DG-03	DG-03.1	Yes
DG-03	DG-03.2	Yes
DG-04	DG-04.1	Yes
DG-04	DG-04.2	Yes
DG-05	DG-05.1	Yes
DG-05	DG-05.2	Yes
DG-06	DG-06.1	Yes
DG-07	DG-07.1	Yes
DG-07	DG-07.2	Yes
DG-08	DG-08.1	Yes
FS-01	FS-01.1	Yes
FS-02	FS-02.1	Yes
FS-03	FS-03.1	Yes
FS-04	FS-04.1	Yes
FS-05	FS-05.1	Yes
FS-06	FS-06.1	Yes
FS-07	FS-07.1	Yes-Conditionally
FS-08	FS-08.1	Yes
FS-08	FS-08.2	Yes
HR-01	HR-01.1	Yes-Conditionally
HR-02	HR-02.1	Yes

HR-02	HR-02.2	Yes
HR-03	HR-03.1	Yes
IS-01	IS-01.1	Yes-Conditionally
IS-02	IS-02.1	Yes-Conditionally
IS-03	IS-03.1	Yes
IS-03	IS-03.2	Yes
IS-03	IS-03.3	Yes
IS-04	IS-04.1	Yes
IS-04	IS-04.2	Yes
IS-04	IS-04.3	Yes
IS-05	IS-05.1	Yes
IS-06	IS-06.1	Yes
IS-06	IS-06.2	Yes
IS-07	IS-07.1	Yes
IS-07	IS-07.2	Yes
IS-08	IS-08.1	Yes
IS-08	IS-08.2	Yes
IS-09	IS-09.1	Yes
IS-09	IS-09.2	Yes
IS-10	IS-10.1	Yes
IS-10	IS-10.2	Yes
IS-10	IS-10.3	Yes
IS-11	IS-11.1	Yes
IS-11	IS-11.2	Yes
IS-12	IS-12.1	Yes
IS-12	IS-12.2	Yes
IS-13	IS-13.1	Yes
IS-14	IS-14.1	Yes
IS-15	IS-15.1	Yes
IS-16	IS-16.1	Yes
IS-16	IS-16.2	Yes
IS-16	IS-16.3	Yes
IS-17	IS-17.1	Yes
IS-17	IS-17.2	Yes
IS-17	IS-17.3	Yes
IS-18	IS-18.1	Yes
IS-18	IS-18.2	Yes
IS-19	IS-19.1	Yes
IS-19	IS-19.2	Yes
IS-19	IS-19.3	Yes
IS-19	IS-19.4	Yes
IS-20	IS-20.1	Yes
IS-20	IS-20.2	Yes
IS-20	IS-20.3	Yes
IS-20	IS-20.4	Yes

IS-20	IS-20.5	Yes
IS-20	IS-20.6	Yes
IS-21	IS-21.1	Yes
IS-21	IS-21.2	Yes
IS-22	IS-22.1	Yes
IS-22	IS-22.2	Yes
IS-22	IS-22.3	Yes
IS-23	IS-23.1	Yes
IS-23	IS-23.2	Yes
IS-24	IS-24.1	Yes
IS-24	IS-24.2	Yes
IS-24	IS-24.3	Yes
IS-24	IS-24.4	Yes
IS-25	IS-25.1	Yes
IS-25	IS-25.2	Yes
IS-26	IS-26.1	Yes
IS-26	IS-26.2	NotAvailable
IS-26	IS-26.3	Yes
IS-27	IS-27.1	Yes
IS-27	IS-27.2	Yes
IS-28	IS-28.1	Yes
IS-28	IS-28.2	Yes
IS-29	IS-29.1	Yes
IS-30	IS-30.1	Yes
IS-31	IS-31.1	Yes
IS-31	IS-31.2	Yes
IS-32	IS-32.1	Yes
IS-33	IS-33.1	Yes
IS-33	IS-33.2	Yes
IS-34	IS-34.1	Yes
IS-34	IS-34.2	Yes
IS-34	IS-34.3	Yes
LG-01	LG-01.1	Yes
LG-02	LG-02.1	Yes
LG-02	LG-02.2	Yes
LG-02	LG-02.3	Yes
OP-01	OP-01.1	Yes
OP-02	OP-02.1	Yes
OP-03	OP-03.1	Yes
OP-03	OP-03.2	Yes
OP-04	OP-04.1	Yes
OP-04	OP-04.2	Yes
OP-04	OP-04.3	Yes
OP-04	OP-04.4	Yes
OP-04	OP-04.5	Yes

RI-01	RI-01.1	Yes
RI-01	RI-01.2	Yes
RI-02	RI-02.1	Yes
RI-02	RI-02.2	Yes
RI-03	RI-03.1	Yes
RI-03	RI-03.2	Yes
RI-04	RI-04.1	Yes
RI-05	RI-05.1	Yes
RI-05	RI-05.2	Yes
RI-05	RI-05.3	Yes
RI-05	RI-05.4	Yes
RI-05	RI-05.5	Yes
RI-05	RI-05.6	Yes
RI-05	RI-05.7	Yes
RM-01	RM-01.1	Yes
RM-02	RM-02.1	Yes
RM-03	RM-03.1	Yes
RM-04	RM-04.1	Yes
RM-04	RM-04.2	Yes
RM-05	RM-05.1	Yes
RS-01	RS-01.1	Yes
RS-02	RS-02.1	Yes
RS-02	RS-02.2	Yes
RS-02	RS-02.3	Yes
RS-03	RS-03.1	Yes
RS-03	RS-03.2	Yes
RS-04	RS-04.1	Yes
RS-05	RS-05.1	Yes
RS-06	RS-06.1	Yes
RS-07	RS-07.1	Yes
RS-08	RS-08.1	Yes
RS-08	RS-08.2	Yes
SA-01	SA-01.1	Yes
SA-02	SA-02.1	Yes
SA-02	SA-02.2	Yes
SA-02	SA-02.3	Yes
SA-02	SA-02.4	Yes
SA-02	SA-02.5	Yes
SA-02	SA-02.6	Yes
SA-02	SA-02.7	Yes
SA-03	SA-03.1	Yes
SA-04	SA-04.1	Yes
SA-04	SA-04.2	Yes
SA-04	SA-04.3	Yes
SA-05	SA-05.1	Yes

SA-06	SA-06.1	Yes
SA-06	SA-06.2	Yes
SA-07	SA-07.1	Yes
SA-08	SA-08.1	Yes
SA-09	SA-09.1	Yes
SA-09	SA-09.2	Yes
SA-09	SA-09.3	Yes
SA-09	SA-09.4	Yes
SA-10	SA-10.1	Yes
SA-10	SA-10.2	Yes
SA-10	SA-10.3	Yes
SA-11	SA-11.1	Yes
SA-12	SA-12.1	Yes
SA-13	SA-13.1	Yes
SA-14	SA-14.1	Yes
SA-14	SA-14.2	Yes
SA-14	SA-14.3	Yes
SA-15	SA-15.1	Yes
SA-15	SA-15.2	Yes

9.2 Cloud DPIA Questionnaire

<u>ID</u>	<u>Question</u>	<u>Explanation</u>	<u>Question type</u>	<u>Response YES</u>	<u>Response NO</u>	<u>Action on YES</u>	<u>Action on NO</u>
<i>Type of project</i>							
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.	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.	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.

2	Do you gather 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 <ul style="list-style-type: none"> - 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 <ul style="list-style-type: none"> - Banking and Financial Management - Payment and Transaction Facilitation - Charitable Donations - Government Services - Healthcare Services - Education Services - Advertising, Marketing, and/or Promotions <ul style="list-style-type: none"> - 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
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	Checkbox <p>Purposes related to the commercial objective of your undertaking</p> <p><i>Health purposes:</i></p> <ul style="list-style-type: none"> - for preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services 		Context specific responses. For instance: employment purposes: The processing of information of employees must be linked to the reason for which	Whichever option, go to the next question	Whichever option, go to the next question

		<p>than processing for exercise of the right to freedom of expression or information.</p>	<ul style="list-style-type: none"> - 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 <p>Employment context:</p> <ul style="list-style-type: none"> - 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 <p>Purposes within the social security context</p> <p>Processing for historical, scientific statistical or research purposes</p> <p>Enforcement of legal claims and/or compliance with law enforcement agencies</p> <p>Exercise of the right to freedom of expression or information (including in the media and the arts)</p> <p>Other (Please specify)</p>		<p>the information was collected for and stay within the context of employment.</p>		
--	--	---	--	--	---	--	--

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	Consent is the weakest ground for a legitimate processing of personal information, and can be withdrawn by the data subject at any time.	Consent is the weakest ground for a legitimate processing of personal information, and can be withdrawn by the data subject at any time.	Go to Question 5	Go to Question 7
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 the mere use of the service or inactivity)			Whichever option, go to the next question	Whichever option, go to the next question
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		The lack of a way, for the data subject, 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
7	Are the consequences of withdrawal of consent significant for individuals?	For instance, will the service to the individual be terminated <i>tout court</i> , while the individual still depends on it?	Y/N			Go to the next question	Go to the next question

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
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

10	Are all the information and its subsets you handle necessary to fulfil 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
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
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 of them.		Go to the next question	Go to the next question
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

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
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 /IDK		The individuals have the right to have their information corrected and updated.	Go to the next question	Go to the next question
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
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	Go to the next question	Go to the next question

					organization/company		
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
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

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
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		A clear communication channel with who acts as DPO enhances transparency and accountability	Go to the next question	Go to the next question
22	Do you appropriately notify your national DPA before performing data processing operations subject to prior checking?	In some cases your processing activities are subject to prior checking by your national DPA.	Y/N	Informing, when necessary, your national DPA about your processing activity is a compliant and transparent attitude	Informing, when necessary, your national DPA about your processing activity is a compliant and transparent attitude	Go to the next question	Go to the next question

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 accordingly.		Go to the next question	Go to the next question
Storage and Security							
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.	Individuals have the right to access the information pertaining to them	Go to the next question	Go to the next question
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
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		Checking the accuracy of information on entry might avoid future costly incidents.	Go to the next question	Go to the next question
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		Outdated information should be rectified or erased because you have an obligation to use current and	If frequently/when requested by the individual/when necessary to comply with	If <i>Rarely or Never</i> , go to the next question

			- Rarely - Never		correct information.	technological developments go to question 29	
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
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	Privacy and data protection legislation is not the only sector you have to consider when assessing the accuracy of the information you process.		Whichever option, go to the next question	Whichever option, go to the next question
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

31	Do you implement any technical and organizational security measure from the outset of your activities?	Think, for instance, whether you are using signatures, hashing, encryption etc. or whether you implement Privacy by Design and/or Privacy by Default mechanisms from the very design phase of your projects.	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
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.	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
33	Is the personnel in your undertaking 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
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
35	Do you adopt one or more of the following	The application of one or more of the following measures may prevent	[Checklist]			Whichever option, go to	Whichever option, go to the next question

	measures and/or procedures as a safeguard or security measure to ensure the protection of personal information?	potential misuse of the information you handle.	<ul style="list-style-type: none"> - 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 			the next question	
--	---	---	--	--	--	-------------------	--

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 may be 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
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		Different kinds of incidents require different kinds of targeted responses.	Go to the next question	N/IDK -> Go to the next question
38	Do you take action in order to notify individuals in case of (security) incidents?	E.g. by sending emails.	Y/N		Notifying individuals in case of incident highly decreases the harms that might derive from it.	Go to the next question	Go to the next question
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	Enacting specific procedures reduces the impact of any unwarranted incident that may happen.	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

			<ul style="list-style-type: none"> - Physical separation of infrastructure - None of the above - Others (please indicate) 				
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		Allowing individuals to set their own retention periods significantly empowers their informational self-determination.	Go to the next question	Go to the next question
41	For how long do you store the information you are dealing with?		[checklist] a) Only for the completion of the project's purposes b) Information is retained for a certain time after the project has been completed c) Information is retained for the possibility of future uses or new purposes d) Until individual requests for erasure			Whichever option, go to the next question	Whichever option, go to the next question
Transfer of information							
42	Do you normally transfer the information you deal with to third parties during your normal processing operations?	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.	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
43	Is the third parties' use compatible with the one you set for your undertaking?	If you transfer information to third parties, do they use the information in a manner consistent with your original purpose(s) and their mandate?	Y/N	You are responsible for the data transfers you enact, even in case of outsourcing.	You are responsible for the data transfers you enact, even in case of outsourcing.	Go to the next question	N/IDK -> Go to the next question

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.	Maintaining the information you process under your direct control reduces the chances of an incident happening	Go to the next question	Go to the next question
45	Are you transferring and/or simply disclosing personal information exclusively to countries or territories outside 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	Countries outside the EEA do not necessarily provide a sufficient level of data protection to the subjects the information relates to		Go to the next question	If N go to 46
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.	These countries, despite being outside the EEA, do provide with a sufficient level of data protection to the subjects the information relates to	These countries, despite being outside the EEA, do provide with a sufficient level of data protection to the subjects the information relates to; the countries outside this list AND outside the EEA do not necessarily provide with an adequate level of protection.	Go to the next question	If N go to the next question

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. Transferring personal information towards countries without an adequate level of protection is a breach of EU data protection laws.	Y/N/IDK	It is mandatory, when transferring information outside the EEA, to do it towards a country provided with an adequate level of protection as defined by European data protection legislation.	It is mandatory, when transferring information outside the EEA, to do it towards a country provided with an adequate level of protection as defined by European data protection legislation.	Go to the next question	N/IDK -> Go to the next question
Cloud Specific Questions							
48	The cloud infrastructure 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)	The higher the number of the subjects who operate in the system, the higher the risk of incidents for its users.	The higher the number of the subjects who operate in the system, the higher the risk of incidents for its users.	Whichever option, go to the next question	Whichever option, go to the next question
49	Does the service provider that you use provide you just with raw computing resources, such as processing capacity or storage, for the information that you process?	Think for instance of Amazon AWS or Microsoft Azure	Y/N	The level of control you have in the cloud has a direct and proportional influence on your level of responsibility.	The level of control you have in the cloud has a direct and proportional influence on your level of responsibility.	Go to the next question	Go to the next question
50	Does the service provider you use provide you with an environment or platform in which you can develop	Think for instance of Google App Engine or Force.com	Y/N	The level of control you have in the cloud has a direct and proportional influence on your level of responsibility.	The level of control you have in the cloud has a direct and proportional influence on your level of responsibility.	Go to the next question	Go to the next question

	and deploy software?				level of responsibility.		
51	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	The level of control you have in the cloud has a direct and proportional influence on your level of responsibility.	The level of control you have in the cloud has a direct and proportional influence on your level of responsibility.	Go to the next question	Go to the next question
52	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 over the information you process. For instance, you can transfer the information you process to another provider if necessary (e.g. in case of 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).	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
53	Does the CSP apply specific procedures in order to secure the information you handle and/or process in case your business is discontinued?	Think, for instance, if the information that you process are preserved in case of merger, acquisition, bankruptcy, etc.	Y/N/IDK		Even if you discontinue your business for whatever reason, the data you dealt with might remain online, with possible negative consequences for the subjects it refers to.	Go to the next question	Go to the next question

54	Does the CSP have an insurance policy against the possible loss or compromise of the information you process in a cloud environment?	Think for instance if the provider is able to redress you in case of unwarranted incidents concerning the information that relates to them through an insurance scheme or similar ones.	Y/N/IDK	Having insurance enhances the possibility that the CSP will be able to provide you with redress if something goes wrong.	Having insurance enhances the possibility that the CSP will be able to provide you with redress if something goes wrong.	Go to the next question	N/IDK -> Go to the next question
55	Does the CSP use resource isolation mechanisms in order to secure the information you entrust it?	Think, for instance, about how the CSP ensures the isolation of your information from the information of other customers potentially located in the same physical machine, albeit of course in a different virtual one.	Y/N/IDK	The centralisation of storage and/or shared tenancy of physical hardware in the cloud environment mean that more individuals are at risk of the disclosure of their information to unwanted parties.	The centralisation of storage and/or shared tenancy of physical hardware in the cloud environment mean that more individuals are at risk of the disclosure of their information to unwanted parties.	Go to the next question	N/IDK -> Go to the next question
56	Are the CSP's activities certified by any kind of supervisory organisation or body?	Think for instance, if the CSP has obtained a certification by a supervisory body or organization, which can guarantee the quality of his services and his compliance with the law.	Y/N/IDK	Certifications often signal the trustworthiness of the provider you are dealing with.	Certifications often signal the trustworthiness of the provider you are dealing with.		

We highlighted in **RED** the answers which carry an off-scale weight and which require a particular and specific consideration.

Methodology

Some answers that the user may give have an influence on the outcome of the DPIA in a way which cannot be reflected by the “incremental” approach we followed and require particular attention and a targeted response and/or advice at the end of the DPIA.

A matrix test follows.

+ L I K E L I H O O D -	Very High	4	5	6	7	8
	High	3	4	5	6	7
	Medium	2	3	4	5	6
	Low	1	2	3	4	5
	Very Low	0	1	2	3	4
		Very Low	Low	Medium	High	Very High
		I M P A C T				

An option could be to calculate (separately) the maximum score in the Impact parameter and the Likelihood parameter that a user could theoretically achieve, and divide that score into five intervals (or into three, if we decide to use a 3x3 matrix), and then assign to each interval a number from 0 to 4 (very low, low, medium, high, very high), which added to the score of the other parameter after the same operation would give us the overall “danger” (risk?) level of the processing activities of the user. Therefore there would be 5 quadrants by 5 quadrants used as means to measure each interval from 0 to 4 (note that “0” is also a quadrant) on the “Likelihood” and “Impact” axis. Since one whole is 100 %, dividing each axis into 5 quadrants would mean that each quadrant on the axis counts for 20 % of the entire axis - thus the 0 quadrant would be from 1 to 20

points scored in the questionnaire, the 1 quadrant would 21 to 40 and so on and so forth. In a hypothetical situation, if the user obtains 18 points on the Likelihood axis, this would place that parameter's overall level under "Low" (so quadrant 1 in the matrix); and she obtains 73 points on the Impact axis, this would place that parameter's overall level under "Very High" (so quadrant 4 in the matrix). With these two results, the overall threat level of the user's processing activities (given to us by the sum of the two parameters) would be 3 on a scale from 0 to 8.

Impact: the incremental impact of the tool's users' activities on the data subject's rights to privacy and data protection.

1. Very low: when the impact of the tool's user's activity would be negligible, if existing, for the data subject.
2. Low: when the impact of the tool's user's activity would be noticeable by the average data subject.
3. Medium: when the impact of the tool's user's activity would sensibly impact the data subject's rights.
4. High: when the impact of the tool's user's activity would be a direct violation of the data subject's rights
5. Very high: when the impact of the tool's user's activity would deprive the data subject of one (or more) of his rights.

Likelihood: the likelihood of an unwarranted incident happening.

We assigned the following weight to the following situations in order to assess it.

1. Very Low: when the harm deriving from the user's activity is *highly unlikely* to happen
2. Low: when the harm deriving from the user's activity is *unlikely* to happen.
3. Medium: when the harm deriving from the user's activity might reasonably happen.
4. High: when the harm deriving from of the user's activity is *likely* to happen
5. Very High: when the harm deriving from the user's activity is *highly likely* to happen.

Risk: The risk is composed by 2 elements: the likelihood of a negative event happening and the impact of the event on the rights of individuals.

The hazards and incidents, which this questionnaire assumes within the concept of risk, are broadly defined as any sensible violation of data protection norms, laws and best practices that could negatively affect either the undertaking, the data subject or both.

9.3 DPIA Screening for Business Use Case 2

<u>ID</u>	<u>Question</u>	<u>Explanation</u>	<u>Question type</u>	<u>Response YES</u>	<u>Response NO</u>	<u>Action on YES</u>	<u>Action on NO</u>	<u>Weight</u>
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	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.	Note

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.	<ul style="list-style-type: none"> - Account and/or Subscription Management - Authentication and Authorization - Customization - Responding to User - (Service) Delivery - Sales of Products or Services - Payment and Transaction Facilitation - Advertising, Marketing, and/or Promotion - State and Session Management 			Whichever option, go to the next question	Whichever option, go to the next question	Note
---	---	---	--	--	--	---	---	------

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		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	For all the fields the likelihood remains the same. However, we valued the impact of health, employment, social security and law enforcement as Very High, for historical, scientific statistical or research purposes as Low, for the exercise of the right to freedom of expression or information as High and for Others as N/A. (+Note)
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			Go to Question 5	Go to Question 7	Impact does not change depending on the answer of the user. If Y- > likelihood is Medium.

5	How have you obtained the consent of individuals?	Consent requires prior information and an explicit indication of the intent to consent.	b) Consent is given directly by the individual by an affirmative action (e.g. by ticking a box)			Whichever option, go to the next question	Whichever option, go to the next question	The impact remains the same. The likelihood ranges: for a) Very Low, for b) Low and for c) Very High (+ note).
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		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-> impact increases to Very High. The likelihood increases to Medium.
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			Go to the next question	Go to the next question	If Y-> Impact and Likelihood increase to Medium.
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.	a) The individual has given his consent			Whichever option, go to the next question	Whichever option, go to the next question	For a) likelihood is Medium For b), c) and d) the impact does not change. The likelihood for b) is Very Low, for c) is Medium and for d) is High For e) likelihood and impact are both Very High.

9	Do you provide clear information about:		<p>the purposes for which you process personal information - Y</p> <p>the different types of information that you process – Y</p> <p>your identity - Y</p>		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 radio button not clicked add 1 to the likelihood.
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		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-> impact and likelihood are High.

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?	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-> impact Very High, likelihood High.
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.	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-> High likelihood, Impact High.
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	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-> impact High, likelihood High.

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	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-> impact High, likelihood High.
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		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-> impact is Very High and likelihood is Very High.

16	Does the information you process about the individual come from different sources?	Think, for instance, whether you obtain databases from other parties	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-> likelihood is Medium, impact does not change
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.	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-> Impact Medium, likelihood Medium.
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.	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-> impact Very High, likelihood High

Storage and Security								
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		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-> impact Very High, likelihood High.
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		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-> impact Very High, likelihood Very High
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.	N			Go to the next question	Go to the next question	If N-> impact High, likelihood High

27	How often is the personal information you process updated?	Outdated information has a negative impact on the accuracy of information you process.	- Frequently - When requested by the individual		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 <i>Rarely or Never</i> , go to the next question	If <i>Rarely or Never</i> -> Impact/likelihood High (+Note for the rest)
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.	- Low			Whichever option, go to the next question	Whichever option, go to the next question	Impact/likelihood depend on the answer (High/Medium/Low/None)
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.	N			Whichever option, go to the next question	Whichever option, go to the next question	Y-> Impact Medium, likelihood does not change N-> Impact/likelihood do not change IDK-> impact does not change, likelihood High
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	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-> likelihood High, impact Medium

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	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-> likelihood Medium, impact Medium
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		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-> impact Medium, likelihood Medium

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		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-> likelihood Medium, impact Medium
34	How often are your Security and Privacy Policies updated?		- Rarely			Whichever option, go to the next question	Whichever option, go to the next question	If <i>Rarely or Never</i> -> Impact/likelihood High (+Note for the rest)

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.	<ul style="list-style-type: none"> - Personal information is kept confidential - Access control is enforced - Segregation of duty is used - Use of personal information are properly documented - 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 - Modalities to express, withhold, or withdraw informed consent to the processing 			Whichever option, go to the next question	Whichever option, go to the next question	Anonymization/ Pseudonymisation and Encryption diminish sensibly the likelihood and the impact of the processing activities (note at the end); the rest of the options diminish them in a minor way. (+Note for the rest options according to the choices of the user)
----	---	--	---	--	--	---	---	---

			- Limitation of usage					
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.	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	<i>Note.</i>

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	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-> likelihood Low, Impact Low
38	Do you take action in order to notify individuals in case of (security) incidents?	E.g. by sending emails.	Y			Go to the next question	Go to the next question	If N-> impact High, likelihood Medium (+Note on data breach)
39	What do you do to minimize the damages of physical, technical and/or security incidents?		<ul style="list-style-type: none"> - Segregation of data bases - Separation on system layer - Multi-tenancy limitations - Physical separation of infrastructure 		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 in likelihood and impact for each box not being ticked.

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.	N			Go to the next question	Go to the next question	If N-> likelihood Low, impact does not change
41	For how long do you store the information you are dealing with?		- 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	Likelihood ranges from Very low to Very High depending on the answer, impact does not change
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		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-> likelihood increases to Medium, Impact does not change.
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			Go to the next question	N/IDK -> Go to the next question	If N-> impact High and likelihood Very High

44	Do you sell, rent or by any means disseminate information to third parties?		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-> impact Medium and likelihood Medium
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.	N			Go to the next question	If not on list go to 47	If Y-> impact Medium and likelihood Very High unless whichever of the options in question 46 are selected.
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	No			Go to the next question	If not on the list -> Go to the next question	
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.	c) is shared amongst multiple users (public cloud)			Whichever option, go to the next question	Whichever option, go to the next question	Note
49	Does the service provider that you use provide you just with raw computing resources, such as processing capacity or storage, for the information that you process?	Think for instance of a provider that provides virtual machines (is that Amazon AWS or Microsoft Azure?)	N		The level of control you have in the cloud has an influence on your responsibility. For instance, if you run your own infrastructure, you are the only one responsible for updating the platforms you use.	Go to the next question	Go to the next question	Note
50	Does the service provider you use provide you with an environment or platform in which you can develop and deploy software?	Think for instance of Google App Engine or Force.com	N			Go to the next question	Go to the next question	Note

51	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			Go to the next question	Go to the next question	Note
52	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		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-> likelihood Very High Impact Very High
53	Does the CSP apply specific procedures in order to secure the information you handle and/or process in case your business is discontinued?	Think, for instance, if the information that you process are preserved in case of merger, partnership, bankruptcy etc.	IDK			Go to the next question	Go to the next question	If N-> Likelihood High, Impact Very High

54	Does the CSP have an insurance policy against the possible loss or compromise of the information you process in a cloud environment?	Think for instance if the provider is able to redress you in case of unwarranted incidents concerning the information that relates to them through an insurance scheme or similar ones.	IDK		Having insurance gives the CSP the certainty to be able to provide you with redress if something goes wrong.	Go to the next question	N/IDK -> Go to the next question	If N → Impact Medium
55	Does the CSP use resource isolation mechanisms in order to secure the information you entrust it?	Think for instance, if the CSP ensures the isolation of your information from the information of other customers potentially located in the same physical machine, albeit of course in a different virtual one.	Y		The centralisation of storage and/or shared tenancy of physical hardware in the cloud environment mean that more individuals are at risk of the disclosure of their information to unwanted parties.	Go to the next question	N/IDK -> Go to the next question	If N-> Impact Very High, likelihood Very High
56	Are the CSP's activities certified by any kind of supervisory organisation or body?	Think for instance, if the CSP has obtained a certification by a supervisory body or organization, which can guarantee the quality of his services and his compliance with the law.	Y					If N-> likelihood Medium.

