cloud security alliance

Privacy Level Agreement Working Group

Privacy Level Agreement [V2]: A Compliance Tool for Providing Cloud Services in the European Union

The PLA-[V2] has been developed within CSA by an expert Working Group composed of representatives of Cloud Service Providers, local Data Protection Authorities and independent security and privacy professionals; co-chaired by Dr. Paolo Balboni and Francoise Gilbert, with the technical supervision of Daniele Catteddu.

May 2015

The PLA working group is sponsored by

EMC² RSA®

Table of Contents

1. Background Information

The Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union (PLA [V1]), was released in February 2013 as a self-regulatory harmonization tool which offers a structured way to communicate the level of personal data protection offered by a cloud service provider (CSP) to customers and potential customers. The PLA [V1] was based not only on EU personal data protection mandatory legal requirements, but also on best practices and recommendations. The PLA [V1] received the endorsement of a number of EU Data Protection Authorities and was used and referenced to develop EU studies, best practices and codes of conduct on personal data protection matters related to cloud computing.

However, after the release of the PLA [V1], the Working Group on PLA realized that CSPs, cloud customers and potential customers still struggle to identify the necessary baseline for personal data protection compliance across the EU with respect to cloud services. Therefore, the Working Group on PLA decided to develop the PLA [V2].

The PLA [V2] is based only on EU personal data protection mandatory legal requirements. Coherently, the Working Group has stripped away elements derived from best practices and recommendations from the PLA [V1] (see further the 'Methodology' section), and further clarifies core mandatory legal requirements.

CAVEAT: the following explanatory note shall be used in conjunction with the Annex 1: PLA V2 Table

2. Objectives

1. PLA [V2] is intended to be used as an appendix to a Cloud Services Agreement, and to describe the level of privacy protection that the CSP will provide. While Service Level Agreements ("SLA") are generally used to provide metrics and other information on the performance of the services, PLAs will address information privacy and personal data[1] protection practices.

2. In a PLA, the CSP would clearly describe the level of privacy and data protection that it undertakes to maintain with respect to the relevant data processing.[2]

3. The adoption of a common structure or outline for these PLAs worldwide can promote a powerful global industry standard, and a self-regulatory harmonization tool may enhance adherence to and with compliance with applicable data protection transparency and accountability obligations.[3]

4. A PLA can offer a clear and effective way to communicate to customers and potential customers the level of data protection offered by a CSP, particularly when transborder data flow issues may arise.[4]

5. Ultimately, the PLA [V2] is intended to provide:

- Cloud customers and potential customers, of any size, with a tool to identify a baseline of mandatory personal data protection legal requirements across the EU and to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions); and
- CSPs, of any size, with guidance to achieve a baseline of compliance with mandatory personal data protection legislation across the EU and disclose, in a structured way, the level of personal data protection that they offer to customers.

[1] "Personal data" or "data" shall mean any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Article 2.a Directive 95/46/EC.

[2] "'Processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Article 2.b Directive 95/46/EC.

[3] PLA [V2] seems to perfectly fit into Key Action 2 "Safe and Fair Contract Terms and Conditions" set forth in the COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Unleashing the Potential of Cloud Computing in Europe. COM(2012) 529 final (European Cloud Strategy): "Identifying and disseminating best practices in respect of model contract terms will accelerate the take up-of cloud computing by increasing the trust of prospective customers. Appropriate actions on contract terms can also help in the crucial area of data protection." (…) "Develop with stakeholders model terms for cloud computing service level agreements for contracts between cloud providers and professional cloud users, taking into account the developing EU acquis in this field." p. 12.

[4] "All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such services. Security, transparency, and legal certainty for the clients should be key drivers behind the offer of cloud computing services." Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ("A.29WP05/2012"), p. 2; "A precondition for relying on cloud computing arrangements is for the controller [cloud client] to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective (…)" p. 4 id. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf)

3. Scope and Methodology

The PLA [V2] only deals with the **Business-to-Business** ('B2B') scenario (as opposed to Business-to-Consumer scenario, 'B2C'), i.e., it considers the case in which the cloud customer is a company.

Within the B2B scenario, the PLA [V2] addresses:

- The situation in which the cloud customer is the data 'controller'[5] and the CSP is a data 'processor'[6]; and
- The situation in which both the cloud customer and the CSP are data controllers.

This feature, which is reflected in the PLA [V2] table in Annex 1, represents an additional added value of PLA [V2], because recent works in this field have limited their scope to the situation in which the cloud customer is the data controller and the CSP is a data processor (e.g., ISO/IEC 27018). The Working Group on PLA is aware of the fact that there may be more complex/hybrid situations (e.g., where the CSP is a joint-data controller), which fall outside the scope of PLA [V2], and recommends the users of the PLA [V2] carefully evaluate the respective privacy roles of the parties involved case-by-case, and to clearly identify related duties and obligations (in this respect the users can refer to Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of "controller" and "processor"[7] 'A.29WP01/2010'). In complex/hybrid situations PLA [V2] may anyway serve as a useful tool to specifically allocate parties' respective duties and obligations that are already clearly listed either under the "CSP is Data Controller" or "CSP is Data Processor" columns of the PLA [V2] table in Annex 1

PLA [V2] remains heavily based on Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing ('A.29WP05/2012'). This landmark opinion is largely and specifically referenced throughout the present document, and is used to anchor PLA [V2] to the mandatory legal provisions of the applicable EU personal data protection framework, i.e., the requirements of 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[8] (Directive 95/46/EC) and its national transpositions.[9] Whereas PLA [V2] aims to be a tool that can be used to achieve/assess baseline compliance with mandatory EU personal data protection legislation horizontally across different sectors and domains, existing EU personal data protection provisions only applicable to specific services (e.g., Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector - Directive on privacy and electronic communications – and subsequent amendments[10]) fall outside the scope of the present work and thus have not been

[5] "'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law." Article 2.d Directive 95/46/EC.

[6] "'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." Article 2.e Directive 95/46/EC.

[7] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[9] EU personal data protection provisions only applicable to specific categories of Directive

[10] Directive 2002/58/EC - available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML - applies to "the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community" (Article 3.1). More precisely, as per Article 1 "Scope and aim 1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic

included as basis for it. The Working Group on PLA recommends that users of PLA [V2] identify possible sector-specific additional requirements to be added on top of PLA [V2]. The PLA [V2] is also written in the light of ISO/IEC 27018[11], the "Cloud Service Level Agreement Standardisation Guidelines"[12], the work developed by the Cloud Select Industry Group on Code of Conduct[13] , and the Cloud Accountability Project[14] .

PLA [V2] is intended to be an EU-wide document, therefore the Working Group on PLA decided to craft a document that potentially should meet ALL requirements of each of the laws of the 28 EU Member States. The Working Group on PLA has thus followed the following methodology, explained here by way of example. PLA [V2] should require a Data Protection Officer (DPO) because some EU countries require a DPO. In other words, if there are countries that require X and other that require Y, this "EU-Wide" document should require the union of X and Y. See in this respect the "Mandatory under EU Data Protection Law" and "Mandatory under only some of the EU Member States laws" columns of the PLA [V2] table in Annex 1.[15]

communication equipment and services in the Community. 2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1."

[11] ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

[12] https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

[13] http://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

[14] http://www.a4cloud.eu/

[15] Please note that specific references to all EU Member States applicable mandatory provisions was beyond the scope and capabilities of the Working Group on PLA [V2]. Where possible, some references have been made, by way of example.

4. Assumptions

Before entering into a contract for the provision of cloud services, a potential cloud customer may consider conducting internal and external due diligence assessment. For example:

- The internal due diligence could be leveraged to identify the restrictions and constraints that might accompany or prevent the potential use of cloud services[16] (e.g., is the cloud a viable solution for the type of data that the entity wishes to process in a cloud?).
- The external due diligence is a reference to determine whether the proposed cloud provider(s) offering(s) meet the potential customer's needs and compliance obligations. It could help to evaluate the level of personal data protection that a CSP would provide. For example, does the proposed CSP provide the level of privacy and data protection, and the level of compliance with applicable laws needed by the company, either because this level has been determined by the company itself, or because it is required by applicable laws?[17]

4.1. Cloud Customer Internal Due Diligence

As part of its internal due diligence, an entity that intends to move personal data to the cloud may consider, among other things:

- Defining its security, privacy and compliance requirements
- Identifying what data / processes / services it will want to move to the cloud
- Reviewing its own internal security and privacy policy and other restrictions on its use of personal data, such as pre-existing contracts, applicable laws and regulations, guidelines and best practices
- Analyzing and assessing the risks
- Identifying which security controls and certifications are required, or are useful, to achieve adequate protection of its employees or customers' personal data while processed in the cloud
- Defining responsibilities and tasks for security controls implementation (i.e., understand which security controls are under the direct governance of the organization, and which security controls would be under the responsibility of the CSP)
- Determining obligations the entity must monitor regarding the activities of its service providers (e.g., are onsite visits required, or is it sufficient to rely on a certification or attestation from a third party?)

[16] For example, the processing of healthcare data in the cloud in Countries such us France should be done only by using services that are certified (i.e., http://esante.gouv.fr/services/referentiels/securite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des)
[17] For more on this issue, see CSA Guidance Version 3 (https://cloudsecurityalliance.org/research/security-guidance/)

4.2. Cloud Customer External Due Diligence

The cloud customer may also consider conducting a due diligence evaluation of the practices of the proposed CSP. This might include, among other things:

- Evaluating whether the CSP fulfills the cloud customer's requirements with respect to privacy and data protection, using the PLA [V2]
- Determining whether the CSP holds any relevant certification or attestation based on an independent third party assessment
- Understanding whether and how to have visibility into, and the ability to monitor, the security controls and practices implemented by the CSP

5. Explanatory Notes

A CSP may offer a variety of PLAs [V2] depending on the type of service provided, the different offerings, or the different practices or markets covered. Moreover, a PLA [V2] may leave room, or point to other documents, for further clarifications of the specific subject and time frame of the cloud service to be provided, and the extent, manner and purpose of the processing of personal data by the CSP, as well as the types of personal data that will be processed. Such information should be gathered and agreed upon with the customer.[18]

To avoid duplication, references can also be made to appropriate provisions in the Master Services Agreement, Service Level Agreement (SLA) or other document that is part of the contract for cloud services. For example, SLAs typically include information about data security. The use of cross-references between documents is intended to simplify things for both clients and CSPs.

The PLA working group is sponsored by EMC.

[18] A.29WP05/2012, Section 3.4.2, p.13.

6. Privacy Level Agreement [V2]*

**** Next to each requirement it is specified:***

[C & P] if the requirement is applicable both to the situation in which the CSP is a controller and the one in which the CSP is a processor;

[C] if the requirement is applicable only to the situation in which the CSP is a controller;

[P] if the requirement is applicable only to the situation in which the CSP is a processor;

6.1. Identity of the CSP (and of Representative in the EU as applicable), its role, and the contact information for the data protection inquiries

Specify:

- CSP name, address, and place of establishment **[C & P]**
- Its local representative(s) (e.g. a local representative in the EU) **[C]**
- Its data protection role in the relevant processing (i.e., controller, joint-controller, processor, or subprocessor)[19] **[C & P]**
- Contact details that the customer can use to submit personal data protection related inquiries **[C & P]**
- Contact details of the Data Protection Officer[20] or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests **[C & P]**
- Contact details of the Information Security Officer or, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests **[C & P]**

[19] A.29WP05/2012 has been written considering the situation in which the customer is a controller and the CSP is a processor, see Section 1, p.4 and Section 3.4. In our opinion the respective roles need to be carefully assessed on a case-by-case basis, as also confirmed by the Information Commissioner's Office in its Guidance on the use of cloud computing ("ICO Guidance"), p. 7. In this respect, see the Sopot Memorandum (http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf?1339501499) adopted by the Berlin International Working Group on Data Protection in Telecommunications in April 2012 ("Sopot Memorandum") p.8 "A commonly recognised data protection principle is that the processor must not process personal data to a greater extent than that which follows from the explicit instructions from the controller. For CC, this implies that a cloud service provider cannot unilaterally make a decision or arrange for personal data (and its processing) to be transmitted more or less automatically to unknown cloud data centers. This is true whether the cloud service provider justifies such a transfer as a reduction of operating costs, management of peak loads (overflow), load balancing, copying to backup, etc. Nor may the cloud service provider use personal data for his own purposes."; A.29WP05/2012 p.23 "The draft proposal clarify that a processor failing to comply with controller's instructions qualifies as a controller and is subject to specific joint controllership rules"; CNIL's Recommendations for companies planning to use Cloud Computing Services ("CNIL's Recommendations", http://www.cnil.fr/fileadmin/documents/en/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf) pp.5-6 "When a customer uses a service provider, it is generally accepted that the former is the data controller and the latter is the data processor. However, CNIL finds that in some cases of public PaaS and SaaS, customers, although responsible for the choice of their service providers, cannot really give them instructions and are not in a position to monitor the effectiveness of the security and confidentiality guarantees given by the service providers. This absence of instructions and monitoring facilities is due particularly to standard offers that cannot be modified by the customers, and to standard contracts that give them no possibility of negotiation. In such situations the service provider could in principle be considered as joint controller pursuant to the definition of "data controller" given in Article 2 of Directive 95/46/EC, since he contributes to the definition of the purposes and means for personal data processing. In cases where there are joint controllers, the responsibilities of each party should be clearly defined." Following the indications of the Italian Data Protection Authority, the CSP is a processor, Cloud Computing: il Vademecum del Garante (http://www.garanteprivacy.it/garante/document?ID=1895296&DOWNLOAD=true) pp.14-15. See also ICO Guidance, pp. 7-9 on the privacy roles in different cloud service deployment models.

[20] See "DPO in Europe: Which countries in Europe have adopted Data Protection Officers?" (http://www.cnil.fr/english/topics/dpo-in-europe/), although it is it is important to point out that this work was carried out by CNIL in March 2012.

6.2. Ways in which the data will be processed

If the CSP is a controller, provide details on (i) the purposes of the processing for which the data are intended and the necessary legal basis to carry out such processing as per Article 7 Directive 95/46/EC[21]; (ii) any further information such as:

- the recipients or categories of recipients of the data,
- the obligatory or voluntary nature of providing the requested data,
- the existence of the right of access to and the right to rectify the data concerning the data subject

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject (Art. 10 Directive 95/46/EC). Distinguish activities that are conducted to provide the agreed cloud service(s) (e.g., storage of data), activities that are conducted at the customer's request (e.g., report preparation or production) and those that are conducted at the CSP's initiative (e.g., back-up, disaster recovery, fraud monitoring). **[C]**

If the CSP is a processor, provide details on the extent and modalities in which the customer-data controller can issue its instructions to the CSP-data processor.[22] **[P]**

Specify how the cloud customer will be informed about relevant changes concerning the relevant cloud service(s) such as the implementation of additional functions.[23] **[C & P]**

[21] Article 7 "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

[22] A.29WP05/2012, Section 3.4.2, p.12. "The agreement should explicitly state that the cloud service provider may not use the controller's data for the cloud service provider's own purposes", Sopot Memorandum, p. 4. See also ICO Guidance, p.12: "The DPA requires the data controller to have a written contract (Schedule 1 Part II paragraph 12(a)(ii)) with the data processor requiring that the "data processor is to act only on instructions from the data controller" and "the data processor will comply with security obligations equivalent to those imposed on the data controller itself." The existence of a written contract should mean that the cloud provider will not be able to change the terms of data processing operations during the lifetime of the contract without the cloud customer's knowledge and agreement. Cloud customers should take care if a cloud provider offers a 'take it or leave it' set of terms and conditions without the opportunity for negotiation. Such contracts may not allow the cloud customer to retain sufficient control over the data in order to fulfil their data protection obligations. Cloud customers must therefore check the terms of service a cloud provider may offer to ensure that they adequately address the risks discussed in this guidance." and p. 17: "The cloud customer should ensure that the cloud provider only processes personal data for the specified purposes. Processing for any additional purposes could breach the first data protection principle. This might be the case if the cloud provider decides to use the data for its own purposes. Contractual arrangements should prevent this."

[23] A.29WP05/2012, Section 3.4.2, p.13. See also the 'Legal' Section of ICO Guidance Checklist, p. 22: "How will the cloud provider communicate changes to the cloud service which may impact on your agreement?". It is worth noticing that CSPs-controllers do not need to have changes approved by customers, whereas, CSPs-processors need to have changes approved by customers, and failure to do so may result in the CSPs acting as controllers (Cfr. A.29WP01/2010').

6.2.1. Personal data location

Specify the location(s) of all data centers where personal data may be processed,[24] and in particular, where and how they may be stored, mirrored, backed-up, and recovered. **[C & P]**

6.2.2. Subcontractors

Identify the subcontractors and subprocessors that participate in the data processing, the chain of accountability and approach used to ensure that data protection requirements are fulfilled.[25] **[C & P]**
Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or subprocessors with the cloud customers retaining at all times the possibility to object to such changes or to terminate the contract.[26] **[C & P]**

6.2.3. Installation of software on cloud customer's system

Indicate whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins) and its implications from a data protection and data security point of view.[27] **[C & P]**

6.3. Data transfer

Indicate whether data is to be transferred, backed-up and/or recovered across borders, in the regular course of operations or in an emergency. If such transfer is restricted under applicable laws, identify the legal ground for the transfer (including onward transfers through several layers of subcontractors)[28]: e.g., European Commission adequacy decision, model contracts,[29] (Safe Harbor[30]) Binding Corporate Rules (BCR)[31]. **[C & P]**

[24] A.29WP05/2012, Section 3.4.1.1, p.11 and Section 3.4.2, p.13. See also the principle of 'location transparency', Sopot Memorandum", p. 4 and CNIL's Recommendations p.14. See also the 'Legal' Section of ICO Guidance Checklist, p. 22, "Which countries will your cloud provider process your data in and what information is available relating to the safeguards in place at these locations? Can you ensure the rights and freedoms of the data subjects are protected? You should ask your cloud provider about the circumstances in which your data may be transferred to other countries. Can your cloud provider limit the transfer of your data to countries that you consider appropriate?"

[25] See the concept of "layered services" in ICO Guidance, pp. 6-8.

[26] A.29WP05/2012, Section 3.3.2, p.10. "There should also be clear obligation of the cloud provider to name al the subcontractors commissioned (e.g., in a public digital register)." A.29WP05/2012, Section 3.4.2, p.13. Cf also A.29WP05/2012 Section 3.4.1.1 pp.10-11, ICO Guidelines, p.11 and Article 10 of the Directive 95/46/EC.

[27] A.29WP05/2012, Section 3.4.1.1, p.11.

[28] See ICO Guidance p.18.

[29] See A29WP05/2012, Section 3.5.3, p.18.

[30] "Adequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the Cloud. Transfers to US organizations adhering to the principles can take place lawfully under EU law since the recipient organizations are deemed to provide an adequate level of protection to the transferred data. However, in the view of the Working Party, sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment. In addition, Article 17 of the EU directive requires a contract to be signed from a controller to a processor for processing purposes, which is confirmed in FAQ 10 of the EU-US Safe Harbor Framework documents. This contract is not subject to prior authorization from the European DPAs. Such contract specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure. Different national legislations and DPAs may have additional requirements. The Working Party considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification. On the contrary, the company exporting data should obtain evidence that the

6.4. Data security measures

Specify the technical, physical and organizational measures in place to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized use, unauthorized modification, disclosure or access and against all other unlawful forms of processing. **[C & P]**

Describe the concrete technical, physical, and organizational measures to ensure:[32] **[C & P]**

- Availability:[33] describe the processes and measures in place to manage the risk of disruption and prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup, restore mechanisms and patch management;[34] **[C & P]**
- Integrity:[35] describe how the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures);[36] **[C & P]**
- Confidentiality:[37] describe how the CSP ensures confidentiality from a technical point of view (e.g., encryption of personal data 'in transit' and 'at rest,'[38] authorization mechanism and strong authentication[39]), and from a

Safe Harbor self-certifications exists and request evidence demonstrating that their principles are complied with. This is important especially with regard to the information provided to data subjects affected by the data processing. The Working Party also considers that cloud client must verify if the standard contracts composed by cloud providers are compliant with national requirements regarding contractual data processing. National legislation may require sub-processing to be defined in the contract, which includes the locations and other data on sub-processors, and traceability of the data. Normally the cloud providers do not offer the client such information – their commitment to the Safe Harbor cannot substitute for the lack of the above guarantees when required by the national legislation. In such cases, the exporter is encouraged to use other legal instruments available, such as standard contractual clauses or BCR. Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC. In terms of data security cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security. Additional safeguards for data security may thus be deployed; such as by incorporating the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes. For these reasons might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud." A29WP05/2012, Section 3.5.1, p.18.

[31] See A29WP05/2012, Section 3.5.4, p.19.

[32] A.29WP05/2012, Section 3.4.2, p.13. See also ICO Guidance, pp. 13-14.

[33] See the 'Availability' Section of ICO Guidance Checklist, p. 22: "Does the cloud provider have sufficient capacity to cope with a high demand from a small number of other cloud customers? How could the actions of other cloud customers or their cloud users impact on your quality of service? Can you guarantee that you will be able to access the data or services when you need them? How will you cover the hardware and connection costs of cloud users accessing the cloud service when away from the office? If there was a major outage at the cloud provider how would this impact on your business?"

[34] A.29WP05/2012, Section 3.4.3.1, p.14.

[35] See the 'Integrity' Section of ICO Guidance Checklist, p. 22: "What audit trails are in place so you can monitor who is accessing which data? Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format. How quickly could the cloud provider restore your data (without alteration) from a back-up if it suffered a major data loss?"

[36] A.29WP05/2012, Section 3.4.3.2, p.15. See also ICO Guidance, p. 22: "Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format."

[37] See the 'Confidentiality' Section of ICO Guidance Checklist, p. 22: Can your cloud provider provide an appropriate third party security assessment? Does this comply with an appropriate industry code of practice or other quality standard? How quickly will the cloud provider react if a security vulnerability is identified in their product? What are the timescales and costs for creating, suspending and deleting accounts? Is all

contractual point of view, such as confidentiality agreements or confidentiality clauses, and company policies and procedures binding upon the CSP and any of its employees (full time, part time, contract employees), and subcontractors (if any), who may be able to access the data and assurance that only authorized persons can have access to data[40] **[C & P]**

- Transparency: describe which technical, physical and organizational measures the CSP has in place to support transparency and to allow review by the customers (see, e.g., Section 5)[41] **[C & P]**
- Isolation (purpose limitation): describe how the CSP provides isolation (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on least privilege principle, hardening of hypervisors[42] and proper management of shared resources wherever virtual machines are used to share physical resources between different cloud customers)[43] **[C & P]**
- Intervenability: describe how the CSP enables data subjects' rights of access, rectification, erasure, blocking and objection; in order to demonstrate the absence of technical and organizational obstacles to these requirements, including cases when data are further processed by subcontractors;[44] (this is also relevant for Section 10) **[C & P]**
- Portability: refer to Section 7
- Accountability: refer to Section 9

---

communication in transit encrypted? Is it appropriate to encrypt your data at rest? What key management is in place? What are the data deletion and retention timescales? Does this include end-of- life destruction? Will the cloud provider delete all of your data securely if you decide to withdraw from the cloud in the future? Find out if your data, or data about your cloud users will be shared with third parties or shared across other services the cloud provider may offer.

[38] Please note that "Encryption of personal data should be used in all cases when 'in transit' and when available to data 'at rest'. (…) Communications between cloud provider and client as well as data centres should be encrypted." A.29WP05/2012, Section 3.4.3.3, p.15. See also ICO Guidance, pp. 14-15.

[39] A.29WP05/2012, Section 3.4.3.3, p.15.

[40] A.29WP05/2012, Section 3.4.2, p.13 and Section 3.4.3.3, p.15. See also ICO Guidance, p. 17.

[41] A.29WP05/2012, Section 3.4.3.4, p.15. Moreover, "Transparency is of key importance for a fair and legitimate processing of personal data. Directive 95/46/EC obliges the cloud client to provide a data subject from whom data relating to himself are collected with information on his identity and the purpose of the processing. The cloud client should also provide any further information such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in so far as such further information is necessary to guarantee fair processing in respect of the data subject (cf. Article 10 of the Directive) Transparency must also be ensured in the relationship(s) between cloud client, cloud provider and subcontractors (if any). The cloud client is only capable of assessing the lawfulness of the processing of personal data in the cloud if the provider informs the client about all relevant issues. A controller contemplating engaging a cloud provider should carefully check the cloud provider's terms and conditions and assess them from a data protection point of view. Transparency in the cloud means it is necessary for the cloud client to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres personal data may be processed at. If the provision of the service requires the installation of software on the cloud client's systems (e.g., browser plug-ins), the cloud provider should as a matter of good practice inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the cloud client should raise this matter ex ante, if it is not addressed sufficiently by the cloud provider." A.29WP05/2012, Section 3.4.1.1, pp.10-11.

[42] "[H]ardening of hypervisors" is also relevant for the 'Integrity' section.

[43] A.29WP05/2012, Section 3.4.3.5, p.16. See also ICO Guidance p. 20.

6.5. Monitoring

Indicate the options that the customer has to monitor and/or audit in order to ensure that appropriate privacy and security measures described in the PLA [V2] are met on an on-going basis. If such monitoring is possible, detail how (e.g., logging, reporting, [first- and/or third-party] auditing[45] of relevant processing operations that are performed by the CSP or the subcontractors).[46] **[C & P]**

6.6. Personal Data breach notification

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a service provided by a CSP.

Specify how the customer will be informed of personal data and data security breaches affecting the customer's data processed by the CSP and/or its subcontractors, within what timeframe and how.[47] **[C & P]**

Specify how the competent Supervisory Authority(ies) and data subjects will be informed of personal data security breaches, within what timeframe and how.[48] **[C]**

6.7. Data portability, migration, and transfer back assistance

Specify the formats, the preservation of logical relations, and any costs associated to portability of data, applications and services.[49] **[C & P]**

[45] Cfr. The 25 August 2014 Decision of CNIL, which evokes the lack of a security audit: http://www.cnil.fr/nc/linstitution/actualite/article/article/la-societe-orange-sanctionnee-pour-defaut-de-securite-des-donnees-dans-le-cadre-de-campagnes/ - http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf.

[46] See A.29WP05/2012, Section 3.4.2, p.13 and Section 3.4.1.2, p.11. See also ICO Guideline, pp. 13.14.

47 In Germany there is a statutory data breach notification requirement that went into effect on September 1, 2009, see Section 42a of the German Federal Data Protection Act. See: Frequently Asked Questions about the German statutory data breach notification requirement: http://www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg. See also A.29WP05/2012, Section 3.4.2, p.13.

48 Id.

[49] Despite the fact that in the actual EU personal data protection legislation there is no explicit provision that set forth a "data portability" obligation, the WG agrees on the significant importance of this provision and suggests to keep it. Moreover, there seems to be enough ground for considering data portability as a mandatory requirement pursuant to general EU personal data protection principles like: "data accuracy" (Article 6.1.d of Directive 95/46/EC), "data availability" and possibility to grant data subjects' rights as per Sections 11.1.c and 12 of Directive 95/46/EC. See also A29WP05/2012, Section 3.4.3.6, p.16 and ICO Guidance, p. 22: "Make sure that the cloud provider allows you to get a copy of your data, at your request, in a usable format. Moreover, see Section 5.4 of the Data Portability of the Cloud Service Level Agreement Standardisation Guidelines:

"5.4. Data Portability

Description of the context or of the requirement

The following list of SLOs is related with the CSP capabilities to export data, so it can still be used by the customer e.g., in the event of terminating the contract.

Description of the need for SLOs, in addition to information available through certification

In related security controls frameworks and certifications the implementation of data portability controls usually focuses on the specification of applicable CSP policies, which makes it difficult (and sometimes impossible) for cloud service customers to extract the specific indicators related

Describe whether, how, and at what cost the CSP will assist customers in the possible migration of the data to another provider or back to an in-house IT environment.[50] **[C & P]**

6.8. Data retention, restitution, and deletion

Describe the CSP's data retention policies and the conditions for returning the personal data and destroying the data once the service is terminated. **[C & P]**

6.8.1. Data retention policy

Indicate for how long the personal data will or may be retained.[51] **[C & P]**

6.8.2. Data retention for compliance with legal requirements

Indicate whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations.[52] **[C & P]**

6.8.3. Data restitution and/or deletion

Indicate the procedure for returning the personal data in a format allowing data portability (see also Section 7), the methods available or used to delete data, and whether data may be retained after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract, and in each case the period during which the CSP will retain the data. **[C & P]**

---

with available formats, interfaces and transfer rates. The following list of SLOs focuses on these three basic aspects of the CSP data portability features, which can be used by the customer e.g., to negotiate the technical features associated with the provider's termination process.
Description of relevant SLOs
Data portability format: specifies the electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service.
Data portability interface: specifies the mechanisms which can be used to transfer cloud service customer data to and from the cloud service. This specification potentially includes the specification of transport protocols and the specification of APIs or of any other mechanism that is supported.
Data transfer rate: refers to the minimum rate at which cloud service customer data can be transferred to/from the cloud service using the mechanism(s) stated in the data interface."

[50] See A.29WP05/2012, Section 3.4.3.6, p.16.

[51] Please note that "[P]ersonal data must be erased [or anonymised] as soon as their retention is not necessary any more." A.29WP05/2012, Section 3.4.1, p.10 and "If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked." Section 3.4.1.3, pp. 11 and "Since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary and even file fragments are to be deleted as well)." Cf also Art.6 of the Directive 95/46/EC. See also A.29WP05/2012, Section 3.4.2, p.13

[52] See ICO Guidance, pp. 16-17.

6.9. Accountability

Describe what policies/procedures the CSP has in place to ensure and demonstrate compliance by the CSP and its subcontractors or business associates, including by way of adoption of internal policies and mechanisms for ensuring such compliance. CSPs need to identify the elements that can be produced and provided as evidence to demonstrate norms' compliance[53] [54] and behaviour. Evidence elements can take different forms, such as attestations, certifications[55], seals, third-party audits[56] attestations[57], logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the (i) Organizational policies level to demonstrate that policies are correct and appropriate; at (ii) IT Controls level, to demonstrate that appropriate controls have been deployed; at iii) Operations level[58], to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to the different levels are privacy seals (i), Certifications like CSA Certification - OCF Level 2 (ii) and logs (iii) produced by reliable monitoring and comprehensive logging mechanisms[59], (iv) audit trails. **[C & P]**

[53] The definition of accountability from the EDPS glossary reads: "Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities." Source: European Data Protection Supervisor (EDPS) (2012), Glossary of terms, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71#accountability.

[54] A.29WP05/2012, section 3.4.4.7, p.16 introduces the notion of (documentary) evidence to be provided to back up the asserted compliance to the data protection principles, "[…] cloud providers should provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles".

[55] E.g., ISO/IEC 27018 and ISO/IEC 27001 certifications, CSA STAR certification.

[56] "Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third-party organisation.45 In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion." See A.29WP05/2012, Section 4.2, p.22.

[57] E.g., SOC 2 attestation, CSA STAR attestation

[58] Evidence at Operations level can be defined as "collection of data, metadata, routine information and formal operations performed on data and metadata which provide attributable and verifiable account of the fulfilment of relevant obligations with respect to the service and that can be used to support an argument shown to a third party about the validity of claims about the appropriate and effective functioning (or not) of an observable system." Source: Wlodarczyk, Pais (eds.), A4Cloud Project Public Deliverable D38.2 "Framework of Evidence", March 2015.

[59] Please note that the CSP may be requested a general obligation to give assurance that its internal organization and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards, as per A.29WP05/2012, Section 3.4.2 p.14. See also Article 17(2) of Directive 95/46/EC and A.29WP05/2012, Section 3.4.3 p.14 and Section 3.4.4.7. See also e.g., CNIL's Recommendations p.12 "a) Observance of French principles on the protection of personal data [The following model clause may be used when the service provider is a data processor] The Parties undertake to collect and process all personal data in compliance with any current regulation applicable to the processing of these data, and in particular with Law 78-17 of 6 January 1978 amended. According to this law, the Customer is data controller for the Processing carried out under the Contract. [The following model clause may be used when the service provider is a joint data controller] The Parties undertake to collect and process all personal data in compliance with any current regulation applicable to the processing of these data, and in particular with Law 78-17 of 6 January 1978 amended. According to this law, the Parties are joint data controllers for the Processing carried out under the Contract."

6.10. Cooperation

Specify how the CSP will cooperate with the cloud customer in order to ensure compliance with applicable data protection provisions, e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights (right of access, correction, erasure, blocking, opposition), to manage incidents including forensic analysis in case of security breach).[60] [See also Section 5: Intervenability and Section 6: Personal data breach notification]. **[C & P]**

Describe how the CSP will make available to the customer and supervisory authorities the information necessary to demonstrate compliance. **[C & P]**

6.11. Legally required disclosure

Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, with special attention to notification procedure to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.[61] **[C & P]**

[60] A.29WP05/2012, Section 3.4.2 p.13. Please note that the CSP is in fact obliged to support the customer in facilitating exercise of data subjects' rights and to ensure that the same holds true for his relation to any subcontractor. A.29WP05/2012, Section 3.4.3.5, p.16.

[61] A.29WP05/2012, Section 3.4.2 pp.13-14. See also extensively Article 29 Data Protection Working Party Opinion 04/2014 on "Surveillance of electronic communications for intelligence and national security purposes" (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf) and ICO Guidance, pp. 19-20.

7. Appendix

	Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws	CSP is Data Controller	CSP is Data Processor
1. IDENTITY OF THE CSP (AND OF REPRESENTATIVE IN THE EU AS APPLICABLE), ITS ROLE, AND THE CONTACT INFORMATION FOR THE DATA PROTECTION INQUIRIES				
Specify:				
CSP name, address, and place of establishment;	Yes		Applicable	Applicable
Its local representative(s) (e.g. a local representative in the EU);	Yes		Applicable	Not Applicable
Its data protection role in the relevant processing (i.e., controller, joint-controller, processor, or subprocessor);	Yes		Applicable	Applicable
Contact details which the customer can use to submit personal data protection related inquiries.	Yes		Applicable	Applicable
Contact details of the Data Protection Officer or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests.		Yes	Applicable	Applicable
Contact details of the Information Security Officer, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests.		Yes	Applicable	Applicable
2. WAYS IN WHICH THE DATA WILL BE PROCESSED				
If the CSP is a controller, provide details on (i) the purposes of the processing for which the data are intended and the necessary legal basis to carry out such processing as per Article 7 Directive 95/46/EC; (ii) any further information such as: - the recipients or categories of recipients of the data, - the obligatory or voluntary nature of providing the requested data, - the existence of the right of access to and the right to rectify the data concerning the data subject in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject (Art. 10 Directive 95/46/EC). Distinguish activities that are conducted to provide the agreed cloud service(s) (e.g., storage of data), activities that are conducted at the customer's request (e.g., report preparation or production) and those that are conducted at the CSP's initiative (e.g., back-up, disaster recovery, fraud monitoring).	Yes		Applicable	Not Applicable
If the CSP is a processor, provide details on the extent and modalities in which the customer-data controller can issue its instructions to the CSP-data processor.	Yes		Not Applicable	Applicable
Specify how the cloud customer will be informed about relevant changes concerning the relevant cloud service(s) such as the implementation of additional functions.	Yes		Applicable	Applicable

	Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws	CSP is Data Controller	CSP is Data Processor
2.1. Personal data location				
Specify the location(s) of all data centers where personal data may be processed, and in particular, where and how they may be stored, mirrored, backed-up, and recovered.	Yes		Applicable	Applicable
2.2. Subcontractors				
Identify the subcontractors and subprocessors that participate in the data processing, the chain of accountability and approach used to ensure that data protection requirements are fulfilled.		Yes	Applicable	Applicable
Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or subprocessors with the cloud customers retaining at all times the possibility to object to such changes or to terminate the contract.		Yes	Applicable	Applicable
2.3. Installation of software on cloud customer's system				
Indicate whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins) and its implications from a data protection and data security point of view.	Yes		Applicable	Applicable
3. DATA TRANSFER				
Indicate whether data is to be transferred, backed-up and/or recovered across borders, in the regular course of operations or in an emergency. If such transfer is restricted under applicable laws, identify the legal ground for the transfer (including onward transfers through several layers of subcontractors): e.g., European Commission adequacy decision, model contracts, Safe Harbor, Binding Corporate Rules (BCR).	Yes		Applicable	Applicable
4. DATA SECURITY MEASURES				
Specify the technical, physical and organizational measures in place to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized use, unauthorized modification, disclosure or access and against all other unlawful forms of processing.	Yes		Applicable	Applicable
Describe the concrete technical, physical, and organizational measures to ensure:	Yes		Applicable	Applicable
Availability: describe the processes and measures in place to manage the risk of disruption and prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup and restore mechanisms;	Yes		Applicable	Applicable
Integrity: describe how the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures);	Yes		Applicable	Applicable

	Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws	CSP is Data Controller	CSP is Data Processor
Confidentiality: describe how the CSP ensures confidentiality from a technical point of view (e.g., encryption of personal data 'in transit' and 'at rest' authorization mechanism and strong authentication), and from a contractual point of view, such as confidentiality agreements or confidentiality clauses, and company policies and procedures binding upon the CSP and any of its employees (full time, part time, contract employees), and subcontractors (if any), who may be able to access the data and assurance that only authorized persons can have access to data;	Yes		Applicable	Applicable
Transparency: describe which technical, physical and organizational measures the CSP has in place to support transparency and to allow review by the customers (see, e.g., Sections 5);	Yes		Applicable	Applicable
Isolation (purpose limitation): describe how the CSP provides isolation (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on least privilege principle, hardening of hypervisors (this is also relevant for the 'Integrity' section) and proper management of shared resources wherever virtual machines are used to share physical resources between different cloud customers);	Yes		Applicable	Applicable
Intervenability: describe how the CSP enables data subjects' rights of access, rectification, erasure, blocking and objection; in order to demonstrate the absence of technical and organizational obstacles to these requirements, including cases when data are further processed by subcontractors (see also Secton 10);	Yes		Applicable	Applicable
5. MONITORING				
Indicate the options that the customer has to monitor and/or audit in order to ensure that appropriate privacy and security measures described in the PLA [V2] are met on an on-going basis.If such monitoring is possible, detail how (e.g., logging, reporting, [first- and/or third-party] auditing of relevant processing operations that are performed by the CSP or the subcontractors).	Yes		Applicable	Applicable
6. PERSONAL DATA BREACH NOTIFICATION **"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a service provided by a CSP**				
Specify how the customer will be informed of personal data and data security breaches affecting the customer's data processed by the CSP and/or its subcontractors, within what timeframe and how.		Yes	Applicable	Applicable
Specify how the competent Supervisory Authority(ies) and data subjects will be informed of personal data security breaches, within what timeframe and how.		Yes	Applicable	Not Applicable

	Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws	CSP is Data Controller	CSP is Data Processor
7. DATA PORTABILITY, MIGRATION, AND TRANSFER BACK ASSISTANCE				
Specify the formats, the preservation of logical relations, and any costs associated to portability of data, applications and services.	Yes		Applicable	Applicable
Describe whether, how, and at what cost the CSP will assist customers in the possible migration of the data to another provider or back to an in-house IT environment.	Yes		Applicable	Applicable
8. DATA RETENTION, RESTITUTION AND DELETION				
Describe the CSP's data retention policies and the conditions for returning the personal data and destroying the data once the service is terminated.	Yes		Applicable	Applicable
8.1. Data retention policy				
Indicate for how long the personal data will or may be retained.	Yes		Applicable	Applicable
8.2. Data retention for compliance with legal requirements				
Indicate whether and how the cloud customer can request the CSP to comply with specific sectoral laws and regulations.	Yes		Applicable	Applicable
8.3. Data restitution and/or deletion				
Indicate the procedure for returning the personal data in a format allowing data portability (see also Section 7), the methods available or used to delete data, and whether data may be retained after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract, and in each case the period during which the CSP will retain the data.	Yes		Applicable	Applicable
9. ACCOUNTABILITY				
Describe what policies/procedures the CSP has in place to ensure and demonstrate compliance by the CSP and its subcontractors or business associates, including by way of adoption of internal policies and mechanisms for ensuring such compliance. CSPs need to identify the elements that can be produced and provided as evidence to demonstrate norms' compliance and behaviour. CSPs need to identify the elements that can be produced and provided as evidence to demonstrate norms' compliance and behaviour. Evidence elements can take different forms, such as attestations, certifications, seals, third-party audits attestations, logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the (i) Organizational policies level to demonstrate that policies are correct and appropriate; at (ii) IT Controls level, to demonstrate that appropriate controls have been deployed; at (iii) Operations level, to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to the different levels are privacy seals (i), Certifications like CSA Certification - OCF Level 2 (ii) and logs (iii) produced by reliable monitoring and comprehensive logging mechanism, (iv) audit trails.	Yes		Applicable	Applicable

	Mandatory under "EU Data Protection Law"	Mandatory under only some of the EU Member State laws	CSP is Data Controller	CSP is Data Processor
10. COOPERATION				
Specify how the CSP will cooperate with the cloud customer in order to ensure compliance with applicable data protection provisions: e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights (right of access, correction, erasure, blocking, opposition), to manage incidents including forensic analysis in case of security breach). [See also Section 4: Intervenability and Section 6: Personal data breach notification].	Yes		Applicable	Applicable
Describe how the CSP will make the information necessary to demonstrate compliance available to the customer and supervisory authorities.	Yes		Applicable	Applicable
11. LEGALLY REQUIRED DISCLOSURE				
Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities; with special attention to notification procedures to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Yes		Applicable	Applicable