cloud security alliance℠

Privacy Level Agreement Working Group

Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union

February 2013

The PLA Outline has been developed within CSA by an expert working group comprised of representatives of cloud service providers, local data protection authorities, and independent security and privacy professionals. The working group is co-chaired by Dr. Paolo Balboni and Francoise Gilbert, with the technical supervision of Daniele Catteddu.

Contents

I. Objectives

1. Privacy Level Agreements (PLAs) are intended to be used as an appendix to Cloud Services Agreements to describe the level of privacy protection that the cloud service provider (CSP) will maintain. While Service Level Agreements (SLAs) 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 it undertakes to maintain with respect to relevant data processing.[2]

3. The adoption of a common structure or outline for these PLAs worldwide can be a powerful global industry standard and a self-regulatory harmonization tool that may enhance adherence to, and 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 data are moved across borders.[4]

---

[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 seems to perfectly fit into Key Action 2 "Safe and Fair Contract Terms and Conditions," as 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.

5. Ultimately, a PLA is intended to provide:

- Cloud customers and potential customers with a tool to assess a CSP's commitment to address information privacy and personal data protection practices (and to support informed decisions);
- CSPs with a tool for structured disclosure of their privacy and data protection practices.[5]

6. This first PLA Outline provides a template for making privacy and data protection disclosures that address the recommendations and guidance provided throughout 2012 by the Article 29 Working Party and several European Data Protection Authorities in a series of seminal papers on cloud contracts and the use of cloud computing services.

II. Assumptions

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

- The internal due diligence could be leveraged to identify the restrictions and constraints that might accompany or prevent the potential use of cloud services (e.g., is the cloud a viable solution for the type of data the entity wishes to process in a cloud?).
- The external due diligence is a reference to determine whether the proposed cloud provider's offerings meet the potential customer's needs and compliance obligations. It could help evaluate the level of personal data protection a CSP would provide (e.g., 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?).[6]

Cloud Customer Internal Due Diligence

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

- Defining its security, privacy and compliance requirements;
- Identifying what data, processes, or services it wants to move to the cloud;

[5] Also pursuant to A.29 WP05/2012.

[6] For more on this issue, see the Cloud Security Alliance Guidance Version 3 at https://cloudsecurityalliance.org/research/security-guidance/

- 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 of moving data to the cloud;
- Identifying what security controls (and certifications) are required or useful to achieve adequate protection of its employees' or customers' personal data while being 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 what obligations the entity has to monitor the activities of its service providers (e.g., are on-site visits required, or is it sufficient to rely on a certification or attestation from a third party?).

Cloud Customer External Due Diligence

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

- Evaluating whether the CSP fulfills the cloud customer's requirements with respect to privacy and data protection using the PLA;
- Checking 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.

III. Explanatory Notes

A CSP may opt to use different PLAs depending on the type of service provided, the different offerings, or the different practices or markets covered. Moreover, a PLA may leave room—or point to another document—for further clarification on the specific subject and time frame of the cloud service to be provided by the CSP, the extent, manner and purpose of personal data processing by the CSP, as well as the types of personal data processed – such information to be gathered and agreed upon with the customer.[7]

To avoid duplication, references can also be made to appropriate provisions in the Master Services Agreement, Service Level Agreement, or other document comprising a cloud services contract. For example, SLAs typically include information about data security. The use of cross-references is intended to avoid redundancy or duplication.

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

IV. Privacy Level Agreement Outline

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

Specify:

- CSP name, address, and place of establishment;
- Its local representative(s) (e.g. a local representative in the EU);
- Its data protection role in the relevant processing (i.e., controller, joint-controller, processor, or subprocessor);[8]
- 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.
- 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.

[8] A.29WP05/2012 has been written considering the situation in which the customer is a controller and the CSP 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 Sopot Memorandum, 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") 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, pp.14-15. See also ICO Guidance, pp. 7-9 on the privacy roles in different cloud service deployment models.

2. Categories of personal data that the customer is prohibited from sending to or processing in the cloud
Specify which categories of personal data the customer is prohibited from sending to or processing in the cloud (e.g., health-related data).

3. Ways in which the data will be processed
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.[9]

If applicable, differentiate between activities conducted on the customer's behalf to provide the agreed cloud service(s) (e.g., storage of data), activities conducted at the customer's request (e.g., report preparation or production), and those conducted at the CSP's initiative (e.g., back-up, disaster recovery, fraud monitoring).

Specify how the cloud customer will be informed about relevant changes concerning applicable cloud service(s), such as the implementation of additional functions.[10]

3.a – Personal data location
Specify the location(s) of all data centers where personal data may be processed,[11] and in particular, where and how they may be stored, mirrored, backed up, and recovered.

---

[9] 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."

[10] 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?"

[11] 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?"

3.b – Subcontractors

Identify the subcontractors and subprocessors participating in the data processing, the chain of accountability, and approach used to ensure that data protection requirements are fulfilled.[12]

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.[13]

3.c – 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 perspective.[14]

4. Data transfer

Indicate whether data might 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).[15]

Indicate whether data is to be transferred outside the European Economic Area. If such transfer takes place, identify on which legal ground: e.g., adequacy decision, model contracts,[16] (Safe Harbor[17]) or Binding Corporate Rules (BCR)[18].

---

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

[13] 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. See 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.

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

[15] See ICO Guidance p.18.

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

[17] "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 Safe Harbor self-certifications exists and

5. 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, modification, disclosure or access, and against all other unlawful forms of processing.

Describe the concrete technical, physical, and organizational measures to ensure:[19]

- Availability:[20] 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;[21]

- Integrity:[22] describe how the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures);[23]

---

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.

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

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

[20] 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?"

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

- Confidentiality:[24] describe how the CSP ensures confidentiality from a technical point of view (e.g., encryption of personal data 'in transit' and 'at rest,'[25] authorization mechanism and strong authentication[26]), and from a contractual point of view, such as confidentiality agreements or confidentiality clauses, as well as company policies and procedures binding upon the CSP and any of its employees (full time, part time, contract employees) and/or subcontractors who may be able to access the data, and assurance that only authorized persons can have access to data;[27]

- 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 6 and 7)[28];

---

[22] 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?"

[23] 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."

[24] 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 its product? What are the timescales and costs for creating, suspending and deleting accounts? Is all 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.

[25] 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.

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

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

[28] 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

- 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, and proper management of shared resources wherever virtual machines are used to share physical resources between different cloud customers)[29];

- 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;[30]

- Portability: refer to Section 9;

- Accountability: refer to Section 11.

Specify which security controls framework(s) is/are in use (e.g., ISO/IEC 27002, CSA CCM, ENISA Information Assurance Framework, etc.) and which specific control is implemented.

6. Monitoring

Indicate whether the customer has the option to monitor and/or audit to ensure appropriate privacy and security measures described in the PLA are met on an ongoing basis. If such monitoring is possible, detail how (e.g., reporting, audit).[31]

Specify the controls that will be given to the customer, as well as the logging and auditing of relevant processing operations performed by the CSP or the subcontractors.[32]

7. Third-party audits

Specify whether and what independent third-party audit reports will be provided to the customer, their scope, the frequency at which these reports will be updated, and whether the full report or a summary of the report will be provided to the client.

---

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.

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

[30] Please also 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. See also ICO Guidance, p. 21.

[31] See A.29WP05/2012, Section 3.4.2, p.13. See also ICO Guideline, pp. 13.14.

[32] See A.29WP05/2012, Section 3.4.1.2, p.11

Specify whether the third-party auditor can be chosen by the customer or chosen by both parties, and who will pay for the cost of the audit.

8. Personal data breach notification

A 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 whether and 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.[33]

9. Data portability, migration, and transfer-back assistance

Specify the formats, the preservation of logical relations, and any costs associated with portability of data, applications and services.[34]

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.[35]

10. 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.

10.a – Data retention policy

Indicate for how long the personal data will or may be retained.[36]

[33] See also A.29WP05/2012, Section 3.4.2, p.13.

[34] See 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."

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

[36] 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)." See also Art.6 of the Directive 95/46/EC. See also A.29WP05/2012, Section 3.4.2, p.13

10.b – Data deletion

Indicate the methods available or employed 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.

10.c – Data retention for compliance with legal requirements

Describe how the CSP satisfies the legal requirements concerning data retention that apply to the CSP and the cloud customer.

Indicate whether and how the cloud customer can request the CSP to comply with specific sectoral laws and regulations.[37]

11. Accountability

Describe what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP and its subcontractors or business associates, including adoption of internal policies and mechanisms for ensuring such compliance, e.g., maintaining documentation of all processing operations under its responsibility and providing reliable monitoring and comprehensive logging mechanisms.[38]

Identify the relevant third-party audit certificates[39] obtained by the CSP, their date and scope.[40]

---

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

[38] 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."

[39] E.g., ISO 27001 certification, SOC 2 attestation, CSA STAR Certification, CSA STAR Attestation.

[40] "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.

12. Cooperation

Specify how the CSP will cooperate with the cloud customer 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, and opposition).[41] [See also Section 5: Intervenability].

Describe how the CSP will make available to the customer and supervisory authorities the information necessary to demonstrate compliance.

13. Law enforcement access

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.[42]

14. Remedies

Indicate what remedies are available to the cloud customer in the event the CSP—and/or the CSP's subcontractors—breaches its contractual obligations under the PLA, such as whether contractual remedies are available for failure to meet data security, monitoring, data breach notification, data portability and/or data retention obligations. Remedies could include compensation for certain types of damages, service credits, and/or contractual penalties (financial or otherwise, including the ability to sue the CSP[43]).

15. Complaint and dispute resolution

Provide the contact details of the CSP representative who will receive questions or complaints regarding the CSP's personal data handling practices.

Provide the contact details of the third party, if any, that may be contacted in order to assist in the resolution of a dispute with the CSP, such as a specific data protection authority, arbitration or mediation service.

16. CSP insurance policy

Describe the scope of the CSP's cyber-insurance policy, if any, including insurance regarding security breaches.

---

[41] 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.

[42] A.29WP05/2012, Section 3.4.2 pp.13-14. See also ICO Guidance, pp. 19-20

[43] A.29WP05/2012, Section 3.4.2 p.12.

V. Annex I to the Privacy Level Agreement Outline

1. IDENTITY OF THE CSP (AND OF REPRESENTATIVE IN THE EU AS APPLICABLE), ITS ROLE, AND THE CONTACT INFORMATION OF THE DATA PROTECTION OFFICER AND THE INFORMATION SECURITY OFFICER	*Specify:* - *CSP name, address, and place of establishment;* - *Its local representative(s) (e.g. a local representative in the EU);* - *Its data protection role in the relevant processing (i.e., controller, joint-controller, processor, or subprocessor);* - *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.* - *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.*
2. CATEGORIES OF PERSONAL DATA THAT THE CUSTOMER IS PROHIBITED FROM SENDING TO OR PROCESSING IN THE CLOUD	*Specify which categories of personal data the customer is prohibited from sending to or processing in the cloud (e.g., health-related data).*
3. WAYS IN WHICH THE DATA WILL BE PROCESSED.	*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.* *If applicable, distinguish activities that are conducted on the customer's behalf 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).* *Specify how the cloud customer will be informed about relevant changes concerning the relevant cloud service(s) such as the implementation of additional functions.* *3.a – 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.* *3.b – 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. *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.* *3.c – 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.*
4. DATA TRANSFER	*Indicate whether data might 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).* *Indicate whether data are to be transferred outside the European Economic Area. If such transfer takes place, identify on which legal ground: e.g., adequacy decision, model contracts, (Safe Harbor) Binding Corporate Rules (BCR).*
5. 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, modification, disclosure or access and against all other unlawful forms of processing.* *Describe the concrete technical, physical, and organizational measures to ensure:* *- 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;* *- Integrity: describe how the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures);* *- 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; - *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 6 and 7) ;* - *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 and proper management of shared resources wherever virtual machines are used to share physical resources between different cloud customers);* - *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;* - *Portability: refer to Section 9;* - *Accountability: refer to Section 11.* *Specify which security controls framework(s) is/are in use (e.g., ISO/IEC 27002, CSA CCM, ENISA Information Assurance Framework, etc.) and which specific control is implemented.*
6. MONITORING	*Indicate whether the customer has the option to monitor and/or audit in order to ensure that appropriate privacy and security measures described in the PLA are met on an on-going basis. If such monitoring is possible, detail how (e.g., reporting, audit).* *Specify the controls that will be given to the customer, as well as the logging and auditing of relevant processing operations that are performed by the CSP or the subcontractors.*

7. THIRD-PARTY AUDITS	*Specify whether and what independent third party audit reports will be provided to the customer, their scope, the frequency at which these reports will be updated, and whether the full report or a summary of the report will be provided to the client.* *Specify whether the third-party auditor can be chosen by the customer or chosen by both parties and who will pay for the cost of the audit.*
8. 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 whether and 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.*
9. 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.* *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.*
10. 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.* *10.a – Data retention policy* *Indicate for how long the personal data will or may be retained.* *10.b – Data deletion* *Indicate 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.*

	10.c – Data retention for compliance with legal requirements *Describe how the CSP satisfies the legal requirements concerning data retention that apply to the CSP and the cloud customer.* *Indicate whether and how the cloud customer can request the CSP to comply with specific sectoral laws and regulations.*
11. 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, e.g., maintaining documentation of all processing operations under its responsibility, providing reliable monitoring and comprehensive logging mechanisms.* *Identify the relevant third party audit certificates obtained by the CSP, their date, and their scope.*
12. 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). [See also Section 5: Intervenability].* *Describe how the CSP will make available to the customer and supervisory authorities the information necessary to demonstrate compliance.*
13. LAW ENFORCEMENT ACCESS	*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.*
14. REMEDIES	*Indicate what remedies are available to the cloud customer in the event the CSP – and/or the CSP's subcontractors – breaches its contractual obligations under the PLA, such as whether contractual remedies are available for failure to meet data security, monitoring, data breach notification, data portability and/or data*

	retention obligations. Remedies could include compensation for certain types of damages, service credits, and/or contractual penalties (financial or otherwise including the ability to sue the CSP).
15. COMPLAINT; DISPUTE RESOLUTION	*Provide the contact details of the CSP representative who will receive questions or complaints regarding the CSP's personal data handling practices.* *Provide the contact details of the third party, if any, that may be contacted in order to assist in the resolution of a dispute with the CSP, such as a specific data protection authority, arbitration or mediation service.*
16. CSP INSURANCE POLICY	*Describe the scope of the CSP's cyber-insurance policy, if any, including insurance regarding security breaches.*

