

|  |
| --- |
| *Privacy Level Agreement Working Group* |
| Privacy Level Agreement  Outline Annex |
| February 2013 |

*The PLA Outline and Annex 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.*

© 2013 Cloud Security Alliance – All Rights Reserved

You may download, store, display on your computer, view, print, and link to this PLA Working Group Privacy Level Agreement Outline available at <https://cloudsecurityalliance.org/pla>, subject to the following.

(a) This PLA Working Group Privacy Level Agreement Outline (February 2013 draft) may be used solely for your personal, informational, non-commercial use; (b) it may not be modified in any way; (c) it may not be redistributed, but you are permitted to link to the document as posted on the <https://cloudsecurityalliance.org/> website; (d) the trademark, copyright or other notices set forth in this document may not be removed, (e) if you, your company, or your organization wishes to make disclosures that follow this Outline, you way use the editable version of the PLA Outline (which is set forth in Annex I to this document, page 16 to 21), which is available at <https://cloudsecurityalliance.org/pla>, as the template for making the disclosures intended by this Privacy Level Agreement Outline.

# 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.* |
|  | |