ECSA
EuroCloud Star Audit
Data Privacy Audit Guide
Table of contents

Introduction .................................................................................................................. 3
ECSA Data Privacy Rules ............................................................................................. 4
Governing Law ............................................................................................................ 6
Sub processing ............................................................................................................ 6
A. TOMs: Cloud Service .............................................................................................. 7
TOMs: Cloud Support ................................................................................................ 11
Introduction

This Audit Guide is a specific directive to deal with

- Contractual and formal requirements according to ECSA Area – 2
- Technical security and data privacy requirements ECSA Area – 3
- Business operation requirement ECSA Area-4

General remarks:

This guide is prepared to reference Cloud Service Providers and Auditors as well as Cloud customer to get familiar with the high level Data Protection requirements on European Level. As main sources the editors used the following public available information by


Please refer also to


Further on it has to be outlined, that most of the European Countries have the own additional Data Privacy Policies which have to be considered for assessment and under the pre-condition that the country of the cloud service customer who is acting as data controller is ruling the requirements and not the location of the Service provider nor the location of the service or data itself.
ECSA Data Privacy Rules

According to EU - Standard Contractual Clauses for Data Processors established in Third Countries

Obligations of the data importer

The data importer agrees and warrants:

(a) To process the personal data only on behalf of the data exporter and in compliance with its instructions and the EU Standard Contractual Clauses. If it cannot provide such compliance, for whatever reason, it agrees to inform the data exporter promptly, of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

(b) That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation, which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will notify the change, to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.
That it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred.

That it will promptly notify the data exporter about:

(i) Any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

(ii) Any accidental or unauthorised access, and

(iii) Any request received directly from the data subjects, without responding to that request, unless it has been otherwise authorised to do so.

To deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data, subject to the transfer, and to abide by the advice of the supervisory authority with regard to the processing of the data transferred.

At the request of the data exporter, to submit its data processing facilities for audit of the processing activities covered by the Clauses. This shall be carried out by the data exporter or an inspection body composed of independent members, in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the data exporter where applicable and in agreement with the supervisory authority.

To make available upon the request of the data subject, a copy of the Clauses or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter.

That, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent.

That the processing services by the sub processor will be carried out.

To send a copy of any sub processor agreement it concludes under the Clauses to the data exporter promptly.
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established

Sub processing

1. The data importer shall not subcontract any of its processing operations, performed on behalf of the data exporter, under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses. Where the sub processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred any further.

---

3 This requirement may be satisfied by the sub processor co-signing the contract entered into between the data exporter and the data importer under this Decision.
The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph

The security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

Security Measures

A. TOMs: Cloud Service

1. Access Control

   Aim: Prevent any unauthorised access; the term is interpreted literally as “to prevent unauthorised persons from gaining access to data processing systems for processing or using personal data."

   Measures: Technical and organisational measures for access control, especially to control the legitimacy of authorised entrants to the facilities and systems where data is stored.

   The CSP takes measures to secure the hosting premises (for example, securing entries and exits) as well as taking measures within the building (for example, alarm systems and restricted access to server rooms) at rented facilities through the use of the following procedures:

   • Established security areas
   • Protection and restriction of access paths
   • Secured decentralized data processing equipment and personal computers
• Established access authorization for employees, including the respective documentation
• Identification of the persons having access authority
• Regulations on key-codes
• Restriction on keys
• Code card passes
• Visitors books (including timekeeping)
• Installation of a security alarm system or other appropriate security measures.

2. System Access Control

Aim: Prevent unauthorized intrusion into computer systems.

Measures: Technical (password / password protection) and organisational (user master record) measures concerning the user identification and authentication:

• The CSP employs industry standard encryption.
• User control shall include the following measures:
  o - Restricted VPN profile
  o - Automatic deactivation of the user ID when several erroneous passwords are entered, log file of events (e.g., monitoring of break-in-attempts)
  o - Issuing of one-time use password controls
  o - Implementation of 2-factor authentication.
• Access control to Customer Data shall include the following measures:
  o - Monitoring capability in respect of individuals who delete, add or modify the exported data
  o - Automatic, system-driven reminders of confidentiality appearing upon each attempt to access systems used in processing data
  o - Effective and measured disciplinary action against individuals who access, or attempt to access data without authorisation.

3. Data Access Control

Aim: Prevent unauthorised activities in computer systems resulting from the exceeding or bypassing of granted permissions. In particular, ensure that persons authorised to use a system have access only to the data they are
authorised to access and that personal data cannot be read, copied, altered or removed without authorisation during processing, use or after recording.

Measures: Demand-driven design approach and the authorisation of access rights, their monitoring and logging through the following:

- The CSP uses a combination of segregation of duties, local access control lists and central logging to ensure data is accessed as authorised and used in an appropriate manner:
  - Intrusion detection systems are installed on both the network and host systems to ensure appropriate access
  - Access controls are reviewed on a periodic basis by both internal and external audits.
- The CSP only uses non-persistent session cookies for authentication and navigation purposes for a user’s session, only.
- The CSP employs industry standard encryption.

4. Data Transmission Control

Aim: Define aspects of data transfer, data transport and transmission control. Ensure that data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or whilst being recorded onto data storage media.

Measures: used in transport, transfer and transmission or storage to disk (manual or electronic) as well as during subsequent controls:

- This shall include measures jointly implemented by both the Customer and the CSP comparable to the following:
  - documentation of the retrieval and transmission of programmes
  - use of encryption
  - monitoring of the completeness and correctness of the transfer of data (success/failure reports will be sent to administrator).

5. Data Input Control

Aim: Ensure the traceability and documentation of data management and maintenance. It should be possible after the fact to check and ascertain whether
personal data have been entered into, altered or removed from data processing systems and, if so, by whom.

Measures: Methods used for subsequent review to reflect whether and by whom data were entered, modified or removed (deleted):

- This shall include measures comparable to the following:
  - Proof established within the CSP’s organisation of the input authorisation
  - Electronic recording of entries (as further specified by the CSP).

6. Job control

**Aim:** Ensure that the instructions of the Customer are fully observed.

Measures: (technical / organisational) on the division of responsibilities between the CSP and Customer:

- Clearly defined responsibilities
- Criteria for selection of the CSP, as determined and communicated by Customer
- Monitoring of execution and performance by reviews of the provided self-certification and audit, as applicable
- Named contacts for submission of change orders.

7. Availability Control

**Aim:** Protect the data against accidental destruction or loss.

Measures: For data storage/backup (physical / logical):

- Documented daily incremental/weekly full backup procedures
- Redundant system infrastructure, Highly-Available Oracle clustering
- Uninterruptible power supply (UPS)
- Separate storage
- Antivirus / firewall
- Emergency plan.
8. Separation control

*Aim: Data collected for different purposes can be processed separately.*

Measures: for separate processing (storage, modification, deletion, transfer) of information with different purposes:

- Functional separation / production / non-production: The CSP maintains complete physical separation between production, development and testing. The customer is provisioned 2 distinct instances: one for production and at least one for non production.
- The customer (including its Affiliates) only has access to the Customer’s instance(s).

**TOMs: Cloud Support**

The following sections define the current security measures. The CSP may improve or increase these at any time. This may mean that individual measures are replaced by new measures that serve the same purpose.

1. Access Control

*Aim: Prevent any unauthorised access; the term is interpreted literally as” to prevent unauthorised persons from gaining access to data processing systems either for processing or using personal data.”*

Measures: The CSP protects its assets and facilities using the appropriate means based on a security classification conducted by an internal security department.

- In general, buildings are secured through access control systems (smart card access system). As a minimum requirement, the outermost shell of the building must be fitted with a certified master key system including modern, active key management.
- Depending on the security classification, buildings, individual areas and surrounding premises will be further protected by additional measures: These include specific access profiles, closed circuit TV, intruder alarm systems, and even biometric access control systems. A separate access control concept, which includes documentation of names, is used in data centers.
- Access rights will be granted to authorised persons on an individual basis according to the defined criteria. This also applies to visitor access. Guests and visitors to CSP buildings must register their names at reception, and must be accompanied by company personnel.
- CSP employees and external personnel must wear their ID cards at all CSP locations.

2. System Access Control

Aim: Prevent unauthorised intrusion into computer systems.

- Measures: Multiple authorisation levels are used to grant access to sensitive systems. Processes are in place to ensure that authorised users have the appropriate authorisation to add, delete, or modify user accounts.
- All users access the CSP's system with a unique identifier (user ID).
- The CSP has procedures in place to ensure that requested authorisation changes are implemented only in accordance with the guidelines (for example, no rights are granted without authorisation). If a user leaves the company, these access rights are rescinded.
- The CSP has a password policy that prohibits the sharing of passwords, governs what to do if a password is disclosed, and requires passwords to be changed on a regular basis. Personalised user IDs are assigned for authentication. All passwords are stored in encrypted form. In the case of domain passwords, the system forces a password change every six months. This complies with the requirements for complex passwords. The CSP ensures that default passwords are changed on networking devices. Each computer has a password protected screensaver.
- The company network is protected from the public network by a hardware firewall. The CSP uses antivirus software at access points to the company network (for e-mail accounts) and on all file servers and all workstations.
- Security-relevant updates for the existing software are regularly and automatically downloaded and installed.
3. Data Access Control

Aim: Prevent unauthorised activities in computer systems resulting from the exceeding or bypassing of granted permissions. In particular, ensure that persons authorised to use a system have access only to the data they are authorised to access and that personal data cannot be read, copied, altered or removed without authorisation during processing, use or after recording.

Measures:

- Access to personal, confidential or sensitive information is granted on a need-to-know basis. In other words, employees or external third parties have access to the information that they require in order to complete their work. The CSP uses authorisation concepts that document how authorisations are assigned and which authorisations are assigned. All personal, confidential, or otherwise sensitive data is protected in accordance with the relevant security standards. Confidential information must be processed confidentially.
- All production servers are operated in the relevant data centers/server rooms. The security systems that protect applications for processing personal, confidential or other sensitive data are regularly checked. To this end, the CSP conducts internal and external security checks and penetration tests on the IT systems.
- The CSP does not permit the installation of personal software or other software not approved by CSP.
- A CSP security standard governs how data and data carriers that are no longer required are deleted or destroyed.

4. Data Transmission Control

Aim: Define aspects of data transfer, data transport and transmission control. Ensure that data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media.

Measures: Data that is transferred from the CSP network to other external networks is encrypted. Where data carriers are physically transported, adequate measures must be taken to ensure the agreed service levels (for example, encryption, lead-lined containers, and so on).
5. Data Input Control

Aim: Ensure the traceability and documentation of data management and maintenance. It should be possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and, if so, by whom.

Measures: The CSP only allows authorised persons to access personal data as required in the course of their work. As part of the support delivery process, the access to customer systems by users and administrators is recorded in a log file.

6. Job Control

Aim: Ensure that the instructions of the Customer are fully observed.

Measures:

- The CSP uses controls and processes to ensure compliance with contracts between the CSP and its service providers.
- As part of the CSP security policy, no customer information is classified lower than “confidential”.
- Access to customer data systems is usually granted via remote support. This is governed by the following security requirements:
- In general, the remote internet connection is established via a Secure Network Communications (SNC) or Virtual Private Networks (VPN) connection. Both options use various security measures to protect customer systems and data from unauthorized access. These include strong encryption, user authentication, and access control technology.
- The Secure Area is a specially designated support ticket facility in which the CSP provides a special access-protected and monitored security area for transferring the access data and password.
- At all times, CSP customers have control over their remote support connections. CSP employees cannot access a customer system without the knowledge or full active support of the customer.
- All CSP employees and contractual partners are contractual bound to respect the confidentiality of all sensitive information including information about the trade secrets of CSP customers and partners.
- During the support process, the personal data of different customers is physically or logically separated.

7. Availability Control

*Aim: Protect the data against accidental destruction or loss.*

*Measures:* The CSP employs backup processes and other measures that ensure rapid restoration of business critical systems as and when necessary. The CSP also uses uninterrupted power supplies (UPS, batteries, generators, and so on) to ensure power is available to the data centers. Emergency processes and systems are regularly tested. Firewalls or other network security technologies are also used. In accordance with the security policy, regularly updated antivirus products are also available on all systems.

8. Separation control

*Aim: Data collected for different purposes can be processed separately.*

*Measures for separate processing (storage, modification, deletion, transfer) of information with different purposes:*

- Functional separation / production / non-production: SAP maintains completely physical separation between production, development and testing. Customer is provisioned 2 distinct instances: one for production and at least one for non-production.
- Customer (including its Affiliates) have access only to Customer’s instance(s).