Security measures on the protection of natural persons with regard to the processing of personal data

This document presents the general description of POST organizational and technical security measures related to personal data processing as part of the execution of contracts with its professional customers

INTRODUCTION

POST implements a reasonable set of technical and organizational measures to ensure an appropriate level of security for personal data that are processed by POST on behalf of the customer. Security measures implemented by POST aim to protect personal data against any security breach resulting, accidentally or unlawfully, in the destruction, loss, alteration, unauthorized disclosure of personal data or unauthorized acces to such data. The level of security implemented depends on each personal data processing, taking into account the nature, scope, context and purposes of the processing, the type of data processed as well as the risks identified for the rights and freedoms of data subjects. This level of security also considers the state of knowledge and the costs of implementation.

1. Measures of pseudonymisation and encryption of personal data

POST is making efforts, as data controllers and/or data processors, in implementing pseudonymisation and / or encryption of personal data by using possible techniques that could fit different scenarios. Each case of personal data processing needs to be analysed, depending on the associated risks, to determine the most suitable technical option in relation to pseudonymisation and encryption of personal data.

Measure identifier	Measure description
1	POST has established a data encryption and key management policy, which defines the requirements when encryption is used and how to protect the cryptographic keys.
2	Creation and validation of a trusted signed certificate to encrypt sensitive data, and secure the HTTPS based web access
3	Secure authentication protocols are used when applicable (FTPS, LDAPS, SSH, etc.)
4	By default, production data with real personal data is not used in test & development environment
5	Pseudonymization techniques are applied through separation of data from direct identifiers to avoid linking to data subject without additional information
6	Full disk encryption is enabled on the workstation operating system drives
7	The use of production data containing personal data or any confidential (C3) or strictly confidential (C4) data is not permitted excepted under the following conditions: • C3 and/or C4 production data is deleted or modified in accordance with ISO/IEC 29101 or • The technical and organisational security measures are identical to those in the production environment. Copying production data to a test environment requires prior authorisation by the business owner of the application. These requests must be documented for audit purposes.
	Related to ISO 27001:2013 - A.15 Cryptography / A.12 Operations security

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

POST is making efforts, as data controllers and/or data processors, in implementing technical and organisational control to ensure ongoing confidentiality, integrity, availability and resilience of data processing systems and services.

Measure identifier	Measure description
1	Database and applications are configured to run using a separate account, with minimum OS privileges to function correctly
2	Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes
3	Encryption solutions are considered on specific files or records through software or hardware implementation
4	Encrypting storage drives are implemented when applicable
5	Employees involved in high risk processing of personal data are bound to specific confidentiality clauses (under their employment contract or other legal act)
6	POST ensures that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process
7	Prior to up taking their duties employees are asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements
8	POST has established the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach)
	Related to ISO 27001:2013 - A.12 Operations security / A.15 Supplier relationships / A.7 Human resource security / A.17 Information security aspects of business continuity management

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

POST implements a backup system for recovery from the loss or destruction of persona data. the frequency and nature of back up will depend on the nature of data being processed. POST complies with the GDPR article 32 on the aspect "ability to restore the availability and access to personal data" as part of the data security obligations for the data controller or data processor.

Measure identifier	Measure description
1	Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities
2	Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data
3	Execution of backups are monitored to ensure completeness
4	Full backups are carried out regularly
5	Backup media are regularly tested to ensure that they can be relied upon for emergency use
6	Scheduled incremental backups are carried out at least on a daily basis
7	Copies of the backup are securely stored in different locations
8	Copies of backups are encrypted and securely stored offline as well
	Related to ISO 27001:2013 - A.12.3 Back-Up

In the event of a personal data security breach, POST asses if this leads to an "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (art. 4(12) GDPR). POST ensures to meet the obligations under articles 33 and 34 GDPR regarding notification of a personal data breach to the supervisory authority and to the data subjects. POST also makes sure to meet their obligation under article 33 GDPR for immediate notification of the data controller. In any case, POST has appropriate procedures in place, not only for the notification of personal data breaches, but also for the overall handling and management of such events.

Measure identifier	Measure description
1	An incident response policy and plans with detailed procedures are defined to ensure effective and orderly response to incidents pertaining personal data
2	Personal data breaches are reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects are in place, following art. 33 and 34 GDPR
3	The incidents' response plan is documented, including a list of possible mitigation actions and clear assignment of roles
4	Incidents and personal data breaches are recorded along with details regarding the event and subsequent mitigation actions performed
	Related to ISO 27001:2013 - A.16 Information security incident management

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Technically, POST undertakes this through a number of technical measures, such as vulnerability scanning, penetration testing, as well as regular security assessment and internal / external audits on critical systems and infrastructure. These are essentially designed to reveal areas of potential risk and things that can be improved.

Measure identifier	Measure description
1	During the development, testing and validation against the implementation of the initial security requirements are performed
2	Vulnerability assessment, application and infrastructure penetration testing are performed if required following the security assessment by CyberForce prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved
3	Software patches should be tested and evaluated before they are installed in an operational environment
4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity referring to POST security policies
5	The security requirements are included in the PPMO (POST Portfolio Management Office), i.e., Security / Privacy by design process and documentations defined at POST group level. Any new project shall follow the security steps for validation.
6	Based on POST information security policies, processes have been implemented, including but not limited to: • Vulnerability and patch management process; • Configuration management process; • Logging and monitoring process; • Logical access management process. KPI and KRI of such processes are reported to the management on regular basis
	Related to ISO 27001:2013 - A.12.6 Technical vulnerability management / A.14.2 Security in development and support processes

5. Measures for user identification and authorisation

POST implements access control and authentication as basic security measures for the protection against unauthorised access to the IT system used for the processing of personal data.

Measure identifier	Measure description
1	Specific access control rights are allocated to each role (involved in the processing of personal data) following the need to know principle (RBAC model)
2	An IAM (Identity and Access Management) system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts
3	The use of generic/shared user accounts is forbidden by default
4	An authentication mechanism is in place, allowing access to the IT system (based on the access control policy and system). As a minimum, a username/password combination are used. Passwords shall respect a certain (configurable) level of complexity following POST Group security policies
5	The access control system has the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity
6	A specific password policy is defined and documented. The policy includes requirements on password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts
7	Segregation of access control roles (e.g. access request, access authorization, access administration) is clearly defined and documented
8	Two-factor authentication is used for all remote access to POST network. The authentication factors include passwords and an OTP (One Time Password)
9	Device authentication is used to guarantee that the processing of personal data is performed only through specific resources in the network
10	Roles with excessive access rights is clearly defined and assigned to limited specific members of staff
11	Access to the IT system is performed only by pre-authorized devices and terminal
	Related to ISO 27001:2013 - A.9 Access control / A.9.1.1 Access control policy

6. Measures for the protection of data during transmission

POST implements network security measures for the protection of personal data, both with regard to external connections (e.g. to the Internet), as well interconnection with other systems (external or internal) of the organization.

Measure identifier	Measure description
1	Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols (TLS/SSL)
2	Wireless access to the IT system is protected by encryption mechanisms
3	Traffic to and from the IT system is monitored and controlled through Firewalls and IDS (Intrusion Detection Systems)
4	The network of the information system is segregated from the other networks of the data controller
	Related to ISO 27001:2013 - A.13 Communications Security / A. 14.1 Security requirements of information systems

7. Measures for the protection of data during storage

POST implements security policies to protect data during storage, including restricting users from performing certain actions that could compromise the security of the IT system (e.g. deactivating of antivirus programs or installation of unauthorised software).

Measure identifier	Measure description
1	Users are not able to deactivate or bypass security settings
2	Anti-virus applications and detection signatures are configured on a daily basis
3	Users do not have privileges to install unauthorized software applications or deactivate installed software
4	The system has session time-outs when the user has not been active for a certain time period
5	Critical security updates are installed regularly following POST Group Security Policies
6	Full disk encryption is enabled on the workstation operating system drives
	Related to ISO 27001:2013 - A. 14.1 Security requirements of information systems

8. Measures for ensuring physical security of locations at which personal data are processed

POST implements physical security measures for office premises as well as the datacenter where personal data is processed.

Measure identifier	Measure description
1	POST has established a physical security policy and has appointed a PSO (Physical Security Officer)
2	Physical access is logged. Regular physical access review and physical security checks are performed by PSO
3	CCTV systems are deployed for premises and datacenter
4	Areas with restricted access are reviewed /checked on regular basis
5	Internal and/or external audits on POST premises and datacenter's physical security measures are performed annually in the context of ISO27001 certification
6	Clear identification, wearing ID Badges, for all personnel and visitors accessing the premises of the organization is established, as appropriate.
7	Secure zones have been defined and are protected by appropriate entry controls. A physical log book or electronic audit trail of all access is securely maintained and monitored
8	Intrusion detection systems are installed in all security zones
9	Physical barriers, where applicable, are be built to prevent unauthorized physical access
10	Vacant secure areas are physically locked and periodically reviewed
11	An automatic fire extinction system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) are implemented at the server rooms
12	External party support service personnel are granted restricted access to secure areas
	Related to ISO 27001:2013 - A.11 – Physical and environmental security

9. Measures for ensuring events logging

The use of log files is an essential security measure that enables identification and tracking of user actions (with regard to the processing of personal data), thus supporting accountability in case of an unauthorised disclosure, modification or destruction of personal data. Monitoring of log files is important for identifying potential internal or external attempts for system violation.

Measure identifier	Measure description
1	Log files are activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion)
2	Log files are timestamped and adequately protected against tampering and unauthorized access. Clocks are synchronised to a single reference time source
3	Actions of the system administrators and system operators, including addition/deletion/change of user rights are logged
4	There are no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity
5	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts
	Related to ISO 27001:2013 – A.12.4 Logging and monitoring

10. Measures for ensuring system configuration, including default configuration

Secure configuration refers to security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities, and prevent of security to prevent any exploit or risk.

Measure identifier	Measure description
1	POST has established a system hardening configuration guideline.
2	POST has implemented configuration management process to ensure secure system configurations
3	The configurations of critical IT systems are regularly reviewed to ensure the compliance with the baseline, standards and best practice.
	Related to ISO 27001:2013 - A.12 Operations Security

11. Measures for internal IT and IT security governance and management

a. Information Security Policies

POST has established an ISMS (Information Security Management System), which includes the information security policy, as well as multiple sub policies for specific domains. A few related processes are also listed in the framework in order to show the compliance to the control requirements of ISO27001:2013.

Measure identifier	Measure description
1	Information security policy and appropriate sub policies are communicated to employees, and interested third parties on need to know basis
2	All the information security policies of POST are reviewed and updated regularly
	Related to ISO 27001:2013 - A.5 Information security policies

b. Organisation of Information Security

Measure identifier	Measure description
1	Information security roles and responsibilities are defined in the Information security policy
2	POST's compliance officer is managing the contact with appropriate authorities for security purposes. POST's data protection officer is managing contact with data protection authority
3	Contact with special interest groups are maintained by different roles within POST, such as compliance officer, information security officer, data protection officer etc.
4	An information security assessment process ('security by design') for new projects and new products have been established to manage the security risks
5	A process of privacy a security by design is defined and applied to new project and product. These processes include risk assessment, penetration test, data protection impact analysis
6	POST has established a risk management policy and procedure to manage operational and security risks. Regular operational and security risk assessments are performed, particularly for critical IT systems / environment
	Related to ISO 27001:2013 - A.6 Organization of information security

c. Human Resource Security

Measure identifier	Measure description
1	POST has implemented HR on-boarding and off-boarding processes for all POST entities, for controls prior to employments
2	Sufficient screening and background check are implemented for new employees
3	New employees receive in the welcome package: • The information security policy • "Sécurité de l'information et la protection des données personnelles" (a booklet) • A leaflet related to POST Telecom specific security requirements (as its status of Support PSF and ISO27001 certified)
4	Employees and sub-contractors of POST are required by the management to comply with established policies and procedures.
5	Compliance checks on the policies and procedures are conducted through different means, such as annual clean desk and clean screen check, KPIs review on security incidents, etc.
6	POST is performing annual security awareness trainings and sessions for all its entities, including POST Telecom. Annual phishing campaigns are implemented to test employee's reaction.
	Related to ISO 27001:2013 - A.7 Human Resource security

12. Measures for certification/assurance of processes and products

POST Telecom is certified ISO 27001:2013 for its Information Security Management System (ISMS), attesting to the high level of maturity of the management and operation processes of its infrastructure dedicated to the provision of managed services (On Premises or in the Cloud), as well as all the support processes inherent to the provision of these services to its customers. The ISO27001 certification demonstrates POST Telecom's expertise in this area, provides customers with a high level of assurance on the security of their managed solutions, as well as high guarantees on the standardisation of POST Telecom's management processes.

13. Measures for ensuring respect of Data Protection principles

Respect for the rights of customers, employees and partners is part of POST's values. In this regard, POST strives to process Personal Data within the strict framework of regulations and with a general ambition of transparency, ethics and respect for privacy. POST had defined several goals in the way Personal Data is processed.

POST undertakes in its Data Protection Policy to process only Personal Data that is appropriate, relevant and strictly necessary for processing for the achievement of their predefined purposes.

a. Privacy by Design/Default

Measure identifier	Measure description
1	POST has deployed a "Privacy by Design" policy for all new products or processing activities involving processing of personal data carried on as Data Processor, to ensure that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is adequate, relevant and necessary for the identified purposes of Data Controller.
2	POST established a global personal data retention policy to ensure data retention periods are limited for the strict necessary period to achieve purposes of its own relevant data processing activities. Retention periods are defined since project phase and based on the purposes and categories of personal data being processed.
3	Mechanisms to correct personal data and to de-identify it when it is no longer needed are considered since project phase.
4	Temporary files created as a result of the processing of Personal Data are disposed of (e.g. erased or destroyed) following documented procedures within a specified, documented period.
5	Personal Data is transferred over data-transmission networks with appropriate controls to ensure that the data reaches its intended destination.
	Related to ISO 27701:2019 - 7.4 Privacy by design and privacy by default / 8.4 Privacy by design and privacy by default

b. Obligations to Data Controllers

Measure identifier	Measure description
1	POST has put in place mechanisms to timely detect Data Breaches.
2	POST has put in place an operational procedure to ensure (potential) Data Breaches are notified to its professional customers as soon as possible.
3	POST has put in place operational procedures to assist its professional customers comply with their obligations as Data Controllers like: • conducting Data Protection Impact Assessments (DPIA); and • assistance in the management of Data Subject Requests
4	At the end of contract, Personal Data is returned to customer and/or disposed in a secure manner.
	Related to ISO 27701:2019 – 8.3 Obligations to PII principals

c. Accountability

Measure identifier	Measure description
1	POST has in place a Data Protection Management System (DPMS) in order to ensure accountability of Personal Data processing activities and controls.
2	POST has documented the processing activities carried out on behalf of its professional customers which include: • categories of processing carried out on behalf of each customer; • transfers to third countries or international organizations; and • a general description of the technical and organizational security measures.
3	POST has documented list of countries and international organizations to which Personal Data can possibly be transferred.
	Related to ISO 27701:2019 – 8.2.6 Records related to processing PII / 8.5 PII sharing, transfer, and disclosure

14. Measures for allowing data portability and ensuring erasure

POST established policies and measures to irreversibly delete or destroy the personal data so that it cannot be recovered. The method(s) used match with the type of storage technology, including paper-based copies. When disposing obsolete or redundant equipment, POST ensures that all data previously stored on the devices has been removed prior to disposal.

Measure identifier	Measure description
1	Software-based overwriting (securely format compliant with POST policy) is performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction is performed
2	Shredding of paper used to store personal data shall be carried out
3	If a third party's services are used to securely dispose of media or paper-based records, a service agreement is in place and a certificate of destruction of records is produced as appropriate
4	Following the software erasure, additional hardware-based measures such as degaussing should be performed. Depending on the case, physical destruction is also be considered.
	Related to ISO 27001:2013 - A. 8.3.2 Disposal of media / A. 11.2.7 Secure disposal or re-use of equipment

15. For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller

Measure identifier	Measure description
1	POST has established a supplier management policy to manage its suppliers and external consultants.
2	All sub-contractors have signed NDAs, which define their responsibilities to protect all POST information (e.g.: personal data, infrastructures…).
3	Sub-contractors follow a security awareness training on annual basis
4	Security requirements on the services outsourced have been defined in the contract between POST and its suppliers. Regular supplier review meetings are organized to managing the services outsourced, including the security aspects
	Related to ISO 27001:2013 - A.15: Supplier Relationships