Positive

Technical and Organisational Measures

April 2026

Introduction

This document describes the arrangements that Positive Group Sales Solutions implements to meet security requirements and cyber security challenges. In particular, it sets out the technical, organisational and procedural measures implemented to maintain the security and protection of data, including personal data in accordance with article 32 of the GDPR.

The Client must ensure that the security measures in place are relevant to the risks associated with its use of the Services.

Evolution of the measures

The technical and organisational measures may evolve at any time. However, such modifications shall not have the purpose of degrading the level of protection of Personal Data.

1. Physical access control to premises and facilities

Appropriate measures to control and prevent physical access by unauthorised persons to premises and facilities.

- Alarm system
- Security personnel, concierges
- Video surveillance installations
- Automatic access control system / Distinction of zones according to risks
- Identification reader by biometrics or by badges, smart cards, magnetic cards, with logging and transponder locking system
- Security locks
- Identity verification
- Visitor registration / accompaniment

Depending on the location and facility, a combination of the above list is in place. It must be taken into account that not all features are present and necessary at all premises or facilities.

2. Access control to data and systems

Appropriate measures to restrict access to systems and data.

- Allocation of user rights based on the principle of least privilege, with review or removal in the event of changes in assignment or departure
- Creation of user profiles:
    - Differentiated access rights (profiles, roles, transactions and objects)
    - Administration of rights by system administrators
- Password procedures (including special characters, minimum length, password change, etc.)
- Authentication with username / password

- Mandatory multi-factor authentication
- Automatic session locking in case of inactivity
- Automatic user account locking after several incorrect access attempts
- Local administration of workstations
- Server administration access via SSM
- Use of secure password managers
- Disk encryption on portable computers
- Encryption of communications
- Use of physical security keys for access to administration interfaces
- Use of anti-virus software / firewalls / restriction of unnecessary services and flows
- Continuous updates of operating systems and applications
- Network segmentation / administration network
- Administrative actions logged and centralised with synchronised time
- Centralisation of application traces on data (access, entries, modifications, deletions)

Depending on the role, the type of software, the level of risk, specific client requirements and necessity, a combination of the measures is in place.

3. Availability control

Measures providing for the availability and protection of data against accidental destruction or loss.

- Backup procedures; backup storage
- Storage of backups in 2 different locations
- Disaster recovery plan (DRP), data duplicated to a secondary site
- Anti-virus systems / firewalls
- Fire and smoke alarm systems
- Automatic fire detection
- Automatic gas extinguishing systems
- Intrusion detection
- Presence of portable and mobile fire extinguishers
- Backup power supply in the event of failure
- Backup Internet link in the event of failure
- Backup air conditioning in the event of failure
- Preventive maintenance plan and tests based on manufacturers' recommendations

Depending on the location and facility, a combination of the above list is in place. It must be taken into account that not all features are present and necessary at all premises or facilities.

4. Segregation control

Measures to provide for separate processing (storage, modification, deletion, transmission) of data for different purposes. Use of dummy data sets outside production systems.

- Separation of test and production systems
- Separation of development and production systems
- Logical separation of client data

5. General internal measures

- Designation of a Data Protection Officer (DPO)
- Periodic evaluation of the measures in place

- Secure file exchange platform
- Procedure for notifying personal data breaches affecting our clients' data
- Procedure for respecting the rights of data subjects in matters of personal data protection
- Confidentiality and personal data protection agreements concluded with personnel
- Awareness-raising actions among personnel from onboarding and on a continuous basis on data protection and security aspects: communication (internal social network, workshops, etc.), training sessions
- Awareness-raising of developers on best practices, code reviews, pair programming
- Sub-processing contracts incorporating personal data protection clauses

6. Infrastructure security and other measures

Measures regarding the continuous security of systems.

- Periodic application security assessments (2 audits per year)
- Limitation of credential stuffing (bruteforce) attacks and rate limiting
- System hardening
- Update plan for production systems
- Continuous vulnerability monitoring (CERT) and deployment of patches according to criticality
- Secure decommissioning process for hardware
- Incident reporting and handling procedure