TOM – Technical and organizational measures

The contracting parties are obliged to define the technical and organisational security measures.

Internal organisation of the contractor

The contractor shall organise its internal organisation in such a way that it meets the special requirements of data protection. In doing so, measures shall be taken that are appropriate depending on the type of personal data or categories of data to be protected.

Concretisation of the individual measures

The requirement are met through the following measures:

1. Confidentiality

1.1. Physical access control

Measures that are suitable for preventing unauthorized persons from accessing data processing systems with which personal data is processed or saved. Xelon AG operates its systems in two independent data centers in Zurich and Aargau (Switzerland):

- GRN: Green Datacenter AG
- NTT: NTT Global Data Centers Switzerland AG

Technical Measures	GRN	NTT
Personnel and goods lock with biometric access control	✓	
Locking system with keys and code lock in our storeroom		✓
Bell system with camera	✓	✓
Badge system with prior identity verification	✓	✓
Alarm system and secured building shafts	✓	✓
Video surveillance of the entrances	✓	✓

Organizational Measures	GRN	NTT
Log of all entries on the personnel and goods lock	✓	✓
Security operations center with security guards	✓	✓
Careful selection of security guards	✓	✓
Log of all entries after identity verification at the security operations center	✓	✓
Key regulation / list of keys	✓	✓
Employee and guest badges	✓	✓
Guests without permanent access only when accompanied by authorized persons	✓	✓
Careful selection of cleaning service employees	✓	✓

1.2. Logical access control

Measures that are suitable to prohibit virtual access to data processing systems by unauthorized persons.

Technical Measures

✓ Login with MFA
✓ Login with SSH keys
✓ Login with username and password
✓ Anti-Virus-Software clients
✓ Firewall
✓ Intrusion Detection System (IDS)
✓ Intrusion Prevention System (IPS)
✓ Use of VPN for remote access
✓ Regular security scan routine

Organizational Measures

✓ Information security policy
✓ User Management
✓ Creation of user profiles
✓ Central password assignment
✓ Secure password policy
✓ Wipe / destroy policy
✓ Clean desk policy
✓ Mobile Device Policy

1.3. Privilege control

Measures that ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data while processing, using and after saving cannot be read, copied, changed or removed without authorization.

Technical Measures

✓ Paper shredder (security level P-1)
✓ Physical wiping of disks
✓ Logging of access to applications, especially during creation, change and removal of data

Organizational Measures

✓ Use of authorization concepts
✓ Minimum number of administrators
✓ Management of user rights by administrators

1.4. Separation Control

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example by logically and physically separating the data.

Technical Measures

✓ Separation of production and test environment
✓ Multi-client capability of relevant applications

Organizational Measures

✓ Control via authorization concept
✓ Defining database rights

1.5. Pseudonymization

The processing of personal data in such a way that the data can no longer be assigned to a specific person without consulting additional information, provided that this additional information is stored separately and is subject to appropriate technical and organizational measures.

Technical Measures

✓ In the case of pseudonymization: Separation of the assignment data and storage in a separate and secure system (encrypted)

Organizational Measures

✓ Internal instruction to anonymize and if possible pseudonymize personal data in the event of disclosure or after the statutory deletion period, respectively our preservation interest, has expired

2. Integrity

2.1. Disclosure control

Measures to ensure that personal data during electronic transmission or during their transport or while saving onto disks can not be unauthorized read, copied, changed or removed and that it can be checked and determined to which external parties a transfer of personal data through facilities for data transmission is intended.

Technical Measures

✓ Use of VPN
✓ Logging of accesses and retrievals
✓ Safe transport containers
✓ Sending over encrypted connections (SFTP, HTTPS)
✓ Usage of signature procedures

Organizational Measures

✓ Documentation and logging of the data recipients as well as the duration of the planned transfer or the deletion periods
✓ Overview of periodical retrieval and transmission processes
✓ Disclosure in anonymous or pseudonymised form if necessary
✓ Careful selection of transport staff and vehicles
✓ Personal delivery with protocol

2.2. Input control

Measures to ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed in data processing systems.

Technical Measures

✓ Technical logging of creation, change and deletion of personal data
✓ Manual control of logs

Organizational Measures

✓ Overview of tools which are used to create, change or delete personal data
✓ Traceability of creation, modification and deletion of data by individual usernames (not user groups)
✓ Assignment of rights to create, modify or deletion of personal data based on an authorization concept
✓ Clear responsibilities for deletions

3. Availability and resilience

3.1. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

Technical Measures

✓ Redundant emergency power systems with diesel generators and batteries operated by DC
✓ Fire and smoke alarm systems
✓ Gas fire extinguishing system
✓ Fire extinguisher server room
✓ Server room monitoring temperature and moisture
✓ Server room redundantly air-conditioned
✓ UPS
✓ Protective power strips server room
✓ Privacy safe
✓ RAID/vSAN system
✓ Video surveillance server room
✓ Alarm message in the event of unauthorized access to the server room

Organizational Measures

✓ Backup & recovery concept
✓ Control of the backup process
✓ Regular data recovery tests and logging of results
✓ Storage of the backup media in a safe place outside the server room
✓ No sanitary connections in or above the server room
✓ Existence of an emergency plan

4. Procedures to periodically review, assess and evaluate

4.1. Privacy management

Data protection encompasses all measures to prevent the undesirable processing of personal data and its consequences.

Technical Measures

- ✓ Central documentation of all procedures and regulations with access options for employees as required / authorized
- ✓ ISO 27001 Information security certification
- ✓ ISO 9001 Quality management certification
- ✓ The effectiveness of the technical protective measures is checked at least once a year

Organizational Measures

- ✓ Internal data protection officer
- ✓ Employees trained and committed to confidentiality / data secrecy
- ✓ Regular security awareness training of employees at least once a year
- ✓ Internal information security officer
- ✓ The data protection impact assessment is carried out if necessary
- ✓ The organization complies with the information obligations under Art. 13 and 14 GDPR
- ✓ Formalized process for processing requests for personal data from those affected

4.2. Incident-Response-Management

Security breach response assistance

Technical Measures

- ✓ Use of firewall with regular updates
- ✓ Use of spam filter with regular updates
- ✓ Use of virus scanner with regular updates
- ✓ Intrusion Detection System (IDS)
- ✓ Intrusion Prevention System (IPS)

Organizational Measures

- ✓ Documented process for detecting and reporting security incidents / data breaches (also with regard to the obligation to report to the supervisory authority)
- ✓ Documented procedure for handling security incidents
- ✓ Involvement of Information security officer and data protection officer in security incidents and data breaches
- ✓ Documentation of security incidents and data breaches using a ticket system
- ✓ Formal process and responsibilities for post-processing of security incidents and data breaches

4.3. Privacy friendly presets

Privacy by design / Privacy by default

Technical Measures

- ✓ No more personal data is collected than is required for the respective purpose
- ✓ Simple exercise of the data subject’s right of withdrawal through technical measures

4.4. Order control (Outsourcing to third parties)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client’s instructions. In addition to data processing on behalf, this item also includes the performance of maintenance and system support work both on site and via remote maintenance.

If the Contractor uses service providers in the sense of commissioned processing, the following points must always be regulated with them.

Organizational Measures

- ✓ Prior verification of the safety measures taken by the contractor and their documentation
- ✓ Selection of the contractor under due diligence aspects (especially with regard to data protection and data security)
- ✓ Conclusion of the necessary agreement on commissioned processing or if need be EU standard contractual clauses
- ✓ Written instructions to the contractor
- ✓ Obligation of the contractor’s employees to maintain data secrecy
- ✓ Obligation to appoint a data protection officer by the contractor if the obligation to appoint exists
- ✓ Agreement on effective control rights vis-à-vis the contractor
- ✓ Regulation on the use of further subcontractors
- ✓ Ensuring the destruction of data after the completion of the order
- ✓ In the case of longer cooperation: Ongoing review of the contractor and its level of protection

Zug, September 2023