TECHNICAL AND ORGANISATIONAL MEASURES (TOM)

BY LIBERA AG (as at 01.09.2023)

1. Data elements used

1.1 Within the framework of the contracts, the client provides LIBERA with personal data and/or confidential data for processing at its own discretion and on its behalf.

1.2 A distinction must be made between personal data and personal data requiring special protection.

Personal data" refers to data relating to an identified or identifiable natural person, i.e. data that allows to draw conclusions about the person's identity.

"Personal data requiring special protection" are categories of personal data that are particularly sensitive personal data, which is why their processing may be subject to special requirements. Sensitive personal data means data among others: data relating to health, data regarding criminal or administrative sanctions, or social assistance.

1.3 Our data processing may concern the following individuals:

- Potential clients, customers, business partners - as individuals.
- Insured individuals who belong to the client's pension solution
- Third parties who are legally associated with those individuals who belong to the client's pension solution

In particular, the following types of personal data may be involved:

- Master data (first name, last name, date of birth, age, gender, nationality, etc.)
- Financial data (remuneration, old age assets, etc.)
- Health data
- Information on social assistance or criminal and administrative sanctions
- Communication data (telephone, e-mail data etc.)

1.4 Data subject to secrecy may, for example, be data subject to professional secrecy, banking secrecy, administrative secrecy or the duty of confidentiality under social security law.

1.5 If the data has been encrypted by the client and is therefore not readable to LIBERA, this does not constitute commissioned data processing by LIBERA. The agreement on commissioned data processing is therefore not applicable to this data.

1.6 The assessment whether the technical and organisational measures described subsequently are appropriate for the protection of the data entrusted to LIBERA for processing (namely in the case of particularly sensitive personal data or data bound to secrecy) is the sole responsibility of the client.

2. Technical and organisational measures

2.1 The following chapters describe the measures taken by LIBERA regarding the protection of personal data in the context of commissioned data processing. The measures listed below are to be understood generically. The following measures apply to cases in which LIBERA itself processes the relevant data. If the data processing is carried out by third parties commissioned by LIBERA, LIBERA will ensure by means of suitable contractual agreements that the third parties comply with comparable measures.

2.2 Access control - Measures suitable for preventing unauthorised persons from gaining access to the data processing systems which are used to process or use personal data:

- Manual locking system
- Security locks
- Key regulation (locking plan)
- Careful selection of cleaning staff
- Selection of employees under due diligence criteria (e.g. professional skills and integrity)

2.3 Access control - measures that prevent data processing systems from being used by unauthorised persons:

- Assignment of user rights
- Establish user profiles
- Password assignment
- Authentication with user name and password
- Access logging (of the users)
- Automatic blocking of clients after a certain time without user activity (password-protected screen saver)
- Use of VPN technology
- Use of two-factor authentication
- Scheduled training to raise security awareness among employees
- Encryption of data medium in laptops
- Use of anti-virus software
- Use of a hardware firewall
- Use of a software firewall
- Regular patching of the infrastructure
- Regular security testing of the infrastructure
- Regular review of the security awareness of employees

2.4 Access control - measures that ensure that only those users authorised to use a data processing system can access the data subject to their access authorisation and that personal data cannot be read, copied, modified, or removed without authorisation during processing, use and after storage:

- Authorisation concept
- Administration of rights by system administrator
- Number of administrators reduced to an inevitable number
- Password policy (password length, password change)
- Physical and non-reversible erasure of data carriers before reuse
- Proper destruction of data carriers
- Use of document shredders by service providers with DIN-66399 certification

2.5 Separation control - measures to ensure that personal data collected for different purposes can be processed separately. Processing is only carried out for the purpose for which the data was collected:

- Separation of productive and test environment
- Physical separation (systems / databases / data carriers)
- Regulation via authorisation concept
- Setting database rights
- Segmentation of the network

2.6 Transfer control - measures to ensure that personal data cannot be read, copied, altered, or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish at which points a transfer of personal data is envisaged by data transmission equipment:

- VPN tunnel facilities
- Use of two-factor authentication
- Transmission of data in encrypted form (M365 Mail encryption)
- Encryption of data carriers in laptops
- Encryption of external data carriers

2.7 Input control - measures that ensure that it can be subsequently verified and established whether and by whom personal data have been processed, modified, or removed from data processing systems:

- Allocation of rights to enter, change and delete data (authorisation concept)
- Server monitoring with logging and event detection
- Logging of all manipulations of data in the pension fund administration system

2.8 Order control (outsourcing to third parties) - Measures that ensure that personal data processed on assignment can only be processed in accordance with the instructions of the outsourcer. In addition to data processing on assignment, this item also includes the performance of maintenance and system support work both on site and via remote maintenance.

LIBERA is entitled to engage subcontracted data processors, provided that they comply with at least the same technical and organisational measures. The IT services used for order processing are managed by various service providers. LIBERA has concluded contractual agreements with all service providers who may have access to personal data.

LIBERA takes the following measures in particular to ensure order control:

- Selection of the contractor under due diligence aspects (especially regarding data protection and data security)
- Conclusion of the necessary agreement on commissioned processing
- Documented instructions to the contractor
- Oblige the contractor to ensure its employees maintain data secrecy
- Rights of control vis-à-vis the contractor
- The same regulations apply to subcontractors of the contractor

2.9 Availability control - measures to ensure that personal data is protected against accidental destruction or loss:

- Uninterruptible Power Supply (UPS)
- Secured access to the server
- Air conditioning in server rooms
- Fire detector with alarm triggering
- No water pipes in or above the server rooms
- Creation of a backup & recovery concept
- Testing of data recovery
- Establishing an emergency plan
- Storage of data backup in a secure, ISO certificated, outsourced location in Switzerland
- Incident response management with defined processing times

3. This version of TOM is a translation of the German version of "Technische und Organisatorische Massnahmen (TOM)". The German version of TOM shall be the binding version and shall be controlling on all questions or interpretations and performance. All translations of the German version of TOM shall be for the convenience of the parties only and shall not be binding upon the parties.