# Technical and Organizational Measures

**DXC Global Privacy and Data Protection Office**
**Applicable Country**: Global

**Effective: 01 June 2022**

**Version: 2.0**

**In accordance with Article 32 of the EU General Data Protection Regulation ("GDPR")**

In the following document are defined the technical and organizational measures ("TOMs") to ensure data protection and data security, which the contractor must at least set up for its own systems and environments and maintain on an ongoing basis. The aim is to ensure, in particular, the confidentiality, integrity and availability of the information processed in the contract.

## 1. Confidentiality

**Access control to the processing areas**

The Contractor shall take the following measures to prevent unauthorized access to the devices used for the processing of personal data.

Depending on the risk group, the facilities are secured by combining different measures, such as:

- Central key management and codes as well as transponder and biometric locks;
- ID card systems with corresponding logging and alarm mechanisms;
- Surveillance by video cameras;
- Round-the-clock reception and visitor policies 7 days a week;
- Security guards;
- Data centers are generally certified according to ISO 27001.

**Access control to data processing systems**

The Contractor shall take the following measures to prevent access to data processing systems by unauthorized persons, such as:

- Individual, identifiable, and role-based assignment of user accounts;
- Defined access permissions for user roles according to the principle "Need-to-Know" and "Least Privilege by Default" (lowest possible rights – data minimization principle);

- Role-based and password-protected access and authorization procedures
  In particular, passwords are:
  - clearly assigned;
  - securely stored and transmitted;
  - sufficiently long and complex design;
  - changed regularly;
  - limited in validity period and initially blocked, in case of inactivity and later deleted;
  - entered manually and, in the event of unauthorized acknowledgement, changed promptly.
- Automatic logout in case of inactivity with re-login for further use of the system;
- Data encryption on the Contractor's mobile devices;
- Deactivation of user accounts after three unsuccessful login attempts;
- All systems are equipped with protection against viruses and spam mails, which is administered centrally.

**Access control to data applications**

The Contractor warrants by the following measures that the persons authorized to use its data processing systems and applications can only access data to the extent and to the extent provided for within the scope of their respective user role/access authorization and that the personal data cannot be read, copied, changed, or deleted without the appropriate permission of the supervisor or a representative:

- Operating system-level authentication;
- Separate authentication at the application level or "single-sign-on" environment;
- Authentication using a centrally managed authentication system (RACF, Active Directory, etc.);
- Division of tasks (technical / organizational – "four-eyes" principle);
- Remote access is only possible via VPN with appropriate authorization and authentication;
- Dedicated access control for all composite systems and storage spaces.

**Separation Control**

The Contractor shall take the following measures to ensure that personal data intended for different purposes can be processed separately:

- Data from different customers is stored physically and/or logically separately from each other (multi-customer systems);
- Access request and authorization processes ensure separate processing of data from different customers or customer areas;
- Separate test and production systems.

**Pseudonymization/Encryption**

The Contractor shall take the following measures to ensure that personal data can only be read by authorized persons:

- Data encryption on all mobile devices and systems of the contractor;
- Data encryption during transmission on the Internet;
- Data encryption for the purpose of authentication (passwords, VPN remote maintenance, etc.);
- Anonymization or pseudonymization on a case-by-case basis, for example to create aggregated data and evaluations.

## 2. Integrity

**Data Forwarding Control**

The Contractor shall take the following measures to prevent personal data from being read, copied, modified or deleted by unauthorized persons during the transmission or transport of the data carriers and shall ensure that it is possible to check and determine to whom personal data should be sent via data transmission devices:

- Firewall Systems, Proxy-Server, NAT Network-Access-Translation;
- Possibility of email encryption and signature;
- Data transfer protocols with encryption of data carriers/media;
- Data transmission via secure data transfer protocols;
- Encrypted VPN (Virtual Private Network) with 2-factor authentication;
- Dispatch of data tapes and other media exclusively by courier in appropriately secured containers, including documentation.

**Input Control**

The Contractor shall take the following measures to check and determine whether and by whom personal data has been entered or deleted from the data processing systems:

- Documentation of administrative activities (setting up user accounts, change management, access and authorization procedures, etc.);
- System log files enabled by default with on-demand control;
- Archiving of password resets and access requests (request/approval process).

## 3. Availability

**Availability control and rapid recovery**

The contractor shall take the following measures to protect personal data from destruction or loss and to ensure a rapid restoration of the operating condition:

- Comprehensive data backup and recovery;
- Disaster recovery and business continuity plans;
- Storage and archiving policies;
- Automatic virus and spam checks, including policies;
- Appropriately equipped data centers, including physically separate alternative data centers if contractually agreed, as well as air conditioning and protection against other harmful environmental and sabotage effects, including:
    - Uninterruptible power supplies;
    - Fully redundant hardware and composite systems, if contractually agreed;
    - Alarm and security systems (smoke, fire, water).

**Data Minimization and Retention**

Contractor shall limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose or to deliver the contracted services. Contractor shall also retain the data only for as long as is necessary taking into account the ongoing validity of the purposes or services for which personal data is processed.

The retention period shall be determined by the following criteria:

- the purpose(s) for which personal data is processed – personal data will be kept for as long as is necessary for that purpose;
- legal obligations – laws or regulations may set a minimum/maximum period for which personal data will have to be kept; and
- contractual obligations – personal data processed by a processor on behalf of a controller will be retained in accordance with the instructions issued by the controller, usually in the form of a contract.

## 4. Procedures for regular review and evaluation

**Data Protection Management**

The Contractor has implemented a privacy organization that operates a privacy management program in accordance with the Company-wide Privacy Policy. This program includes the following 10 program elements:

- Organization and strategy;
- Data and risk assessment;
- Inventory of applicable legal regulations;
- Policies and Processes;
- Information Security Management System (ISMS);
- Training;
- Data transfer protocol;
- Supplier Management;
- Incident Management;
- Monitoring and control;

**Incident Management**

The Contractor has implemented a suitable system for the management of security incidents, which also handles privacy/data protection incidents and their consequences. This is done in cooperation with the IT security department and legal department and includes:

- IT incident management covers the entire organizational and technical process of responding to detected or suspected security incidents or incidents. Disruptions in IT areas as well as preparatory measures and processes;
- Treatment of legal, including contractual aspects under data protection law, reporting and information obligations.

**Privacy-friendly presets and technology design**

The Contractor shall take appropriate technical and organizational measures to ensure that, by default, only personal data whose processing is necessary for the respective specific processing purpose are processed. These principles apply to:

- the amount of personal data collected,
- the scope of their processing,
- their storage period, and
- their accessibility.

The following principles serve to ensure that personal data are not made accessible to an indefinite number of natural persons by default without the intervention of an individual:

- *Necessity principle:* Access authorizations are granted by default according to the principles "need-to-know" and "need-to-do";
- *Data minimization/data economy:* The provider collects and processes only personal data within the scope of its contractually agreed lines that are necessary for the fulfillment and exercise of the services.

**Order Control**

The Contractor shall take the following measures to ensure that personal data are processed only in accordance with the agreement and the instructions of the Client:

- The service contracts contain corresponding requirements and obligations, such as the client's right to issue instructions as well as corresponding mechanisms and controls;
- Contractual provisions, such as EU standard contractual clauses;
- Control rights of the client;
- Use of subcontractors only in accordance with contractual agreements.

## 5. DATA CENTER / DELIVERY CENTER

DXC maintains a formal Information Security Management System (ISMS) that achieved formal certification as defined in ISO/IES 27001 for all its Data and Delivery centers which follows a continual cycle of improvement to ensure that best practices are documented and reinforced.

Moreover, DXC maintains a formal Privacy Information Management System (PIMS) that achieved formal certification as defined in ISO/IES 27701 for its global and regional delivery centers.

## 6. CLIENT SECURITY PRINCIPLES

DXC maintains the client’s security requirements as specified within the client services agreement.