DXC TECHNOLOGY

DXC Integrity

GLOBAL DATA PROTECTION

DXC Public

Technical and Organizational Measures

TECHNICAL AND ORGANIZATIONAL MEASURES

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

1. Confidentiality

Access Control to the Processing Areas
DXC 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; and
- Security guards.

Access Control to Data Processing Systems
DXC 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
  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; and
  - 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 DXC's mobile devices;
- Deactivation of user accounts after three unsuccessful login attempts; and
- All systems are equipped with protection against viruses and spam mails, which is administered centrally.

Access Control to Data Applications
DXC warrants by the following measures that the persons authorized to use its data processing systems and applications can only access data 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; and
- Dedicated access control for all composite systems and storage spaces.

Separation Control
DXC 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; and
- Separate test and production systems.

Pseudonymization/Encryption
DXC shall take the following measures to ensure that only authorized persons can read personal data:

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

Privacy-Friendly Presets and Technology Design
DXC 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:

- Amount of personal data collected,
- 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
DXC shall take the following measures to ensure that personal data are processed only in accordance with the agreement and the instructions of the customer:

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

2. Integrity

Data Forwarding Control
DXC 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; and
- Dispatch of data tapes and other media exclusively by courier in appropriately secured containers, including documentation.

Input Control
DXC 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; and
- Archiving of password resets and access requests (request/approval process).

3. Availability

Availability Control and Rapid Recovery
DXC 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; and
- 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; and
  - Alarm and security systems (smoke, fire, water).

Data Minimization and Retention
DXC 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. DXC shall also retain the data only for as long as is necessary considering 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
DXC has implemented a Global Data Protection (GDP) organization that operates a GDP Program in accordance with DXC's Global Privacy and Data Protection Policy. This GDP Program includes the following ten program elements:

Governance and Organization
DXC has chartered, and will maintain, the GDP Program to manage and oversee all matters related to privacy and data protection. The GDP Program is integrated within DXC Integrity, the corporate ethics and compliance function.

Data and Risk Assessment
Global Data Protection uses privacy assessments to ensure compliance with global data protection laws. Where necessary and to the extent required by applicable laws, a privacy assessment will determine whether the processing of personal data poses a risk to an individual's right to privacy.

Inventory of Applicable Laws and Regulations

DXC processes personal data only as permitted or required by applicable data protection laws.

Policies and Procedures

DXC maintains policies and procedures subject to annual review to ensure a uniform, consistent and cohesive approach to the collection, use, transfer, storage and destruction of personal data.

Information Security Protocols

DXC takes all legally required and commercially reasonable measures, proportionate to the associated risk, to protect personal data from loss, misuse, unauthorized access or disclosure, alteration or destruction. DXC provides appropriate additional levels of protection for data considered to be sensitive personal data.

Training and Awareness Programs

DXC is committed to implementing education and awareness initiatives that help to build the knowledge and skills necessary to promote individual and collective responsibility for protecting personal data. These initiatives align with legal, regulatory and contractual requirements.

Data Transfer Protocols

DXC adequately protects personal data that is disclosed to a third party or transferred to or accessed from another country. This includes internal transfers within DXC or between DXC business units and/or third parties. Protective measures may be ensured contractually or otherwise.

Third-Party Compliance Processes

Due diligence of all potential third parties should be carried out prior to the selection and initiation of a contract or relationship.

Data Breach Incident Plan

DXC 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, disruptions in IT areas as well as preparatory measures and processes; and
- Treatment of legal and contractual aspects under data protection laws and reporting obligations.

Ongoing Auditing and Monitoring

DXC designates suitably qualified individuals to be responsible and accountable for managing and overseeing the protection of personal data, using internal controls based on privacy principles. These individuals do the following:

- Provide support to any audit bodies or regulators if required by specific standard or regulation;
- Carry out regular internal GDP Program effectiveness assessments and create respective GDP Program metrics and reports;
- Maintenance of a risk-based audit plan that determines effectiveness of internal controls, policies and procedures regarding, for example, privacy impact assessment, due diligence and vendor/supplier compliance.
- The audit plan focuses on high-risk areas and areas subject to legal audit requirements. The audit plan determines the scope of the audit and defines the processes and procedures for managing the audit outcome.
- A data protection audit in combination with pro-active, regular, as well as case-based, privacy compliance reviews is essential to identify and mitigate potential weaknesses before they become major problems.

The above-mentioned internal controls reflect the actual review approaches taken in relation to the ten GDP Program elements, as monitoring is the program element that serves review purposes.

5. Data Center/Delivery Center

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

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

6. Customer Security Principles

DXC maintains the customer's security requirements as specified within the customer services agreement.