Privacy Statement of DXC

Statement regarding Processing of Personal Data according to the EU General Data Protection Regulation in the framework of accessing the CDX system

(1) Introduction, Scope, Definitions

This Privacy Statement of DXC regulates the rights and obligations of CLIENT (in the following the "Controller") and the EntServ Deutschland GmbH (in the following "DXC" or "Processor") as part of the processing of personal data by Processor. The subject matter of this Privacy Statement of DXC results from the use of the platform CDX by accepting the Terms of Use and accessing the CDX application. Before mentioned roles and responsibilities are defined in the Terms of Use.

This Privacy Statement of DXC applies to all activities where employees of Processor or its subcontractors process personal data of Controller.

Terms used in this Privacy Statement of DXC are to be construed according to their definition in the EU General Data Protection Regulation.

Instructions or explanations regarding Data Privacy shall be basically given in writing. In exceptional cases, instructions and explanations can also be given in another form, if an appropriate proof is ensured.

(2) Subject Matter and Duration of Processing

a) Subject Matter

Processor shall process the following data:

- Processor only uses the personal data for the purpose of internal user administration.
- The user administration fulfils essential security requirements for logging and controlling access to the system.

The Controller acknowledge that the service in general is a web-based (= Internet) self-service system for exchanging material data. The Data Controller will in his own authority

- attach personal data, e.g. name and telephone of contact persons, in the Material Data Sheet;
- publish and distribute Material Data Sheet in the system (including as the case may be personal data like the before mentioned data of the contact person) and
- therefore, grant other companies and/or user access to the Material Data Sheets showing – as the case may be – personal data of the Data Controller.

Furthermore, the Controller respectively USER acknowledge that it is not possible to withdraw Material Data Sheets by an automatic process when the Data Sheets were published or distributed to the systems of another company or USER.

b) Duration

Processing will start at the time when the USER respectively the CLIENT accepts the Terms of Use and will go on for an indefinite period of time until the Contract will be terminated by one of the Parties of the License Agreement respectively USER wants to terminate his account.

(3) Type and Purpose of Data Collection, Processing or Use:

a) Type and Purpose of Processing

The data will be processed as follows:

- user administration
- contact data

The purpose of processing is as follows: See above subsection (2) “Subject Matter and Duration of Processing”.

b) Type of Data

The following types of data will be processed:

- User Administration
  - Name (first name / last name)
  - Communication data (e.g., phone, email)
  - Contract master data (contractual relationship, product and/or contractual interest)
  - Billing and payment data (as the case may be credit card information)
- Contact Information with Material Data Sheet

c) Categories of Persons Affected

The following persons will be affected by the processing of data:

- Customers (CLIENT)
- Subscribers (USER)
- Employees / staff
- Suppliers
- Contacts

(4) Processor Obligations

Processor only processes personal data to the extent required for fulfilling the Terms of Use, unless Processor is legally obligated to process the data otherwise. If Processor is subjected to such obligation, Processor shall inform Controller accordingly prior to data processing, unless prohibited by law to communicate such information.

Processor acknowledges that it is aware of the pertinent general data protection regulations and that it shall observe the principles of proper data processing. Processor undertakes to observe strict secrecy when processing the data.

Individuals involved by Processor that might obtain knowledge of the data to be processed shall receive appropriate privacy and data protection training and shall be bound to secrecy in writing, unless already obligated to maintain secrecy by virtue of statutory regulations or any other pertinent obligation.

Taking into account the nature of the processing, Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising data subject's rights. Any data subject requests directly addressed to Processor shall be immediately forwarded to Controller.

Processor has appointed a Data Protection Officer who can be contacted via e-mail at:

(5) Transfer of Personal Data

Personal data submitted to CDX will be processed by Processor on platforms operated within the European Union (EU) or within the European Economic Area (EEA) exclusively. Any relocation to a non-EU country will be communicated accordingly and is subject to the provisions of the EU General Data Protection Regulation set forth in Section V – "Transfer of Personal Data to non-EU Countries" and subject to compliance with the provisions of the Terms and Conditions.

(6) Personal Data Protection

a) General Requirements

The data security measures described below in Section 6 b) are implemented and maintained by Processor to ensure an adequate level of data protection and data security in terms of confidentiality, integrity and availability of the processed data.

The data security measures will be subject to technological progress to ensure continued adequate level of protection and may be implemented without prior notice, unless otherwise agreed in any client-specific contract. Copies or duplicates of personal data are only made for technical purposes and as far as it is required for DXC to meet its legal and contractual obligations.

Processor regularly furnishes proof of meeting its obligations, including but not limited to the full implementation of the agreed technical and organizational measures.

b) Technical and Organizational Measures

Control of Access to Processing Sites

Processor shall implement the below listed measures to prevent unauthorized access to the devices used for the processing of personal data.

Depending on the risk category, the facilities shall be secured by a combination of different measures, such as

- Central key management and codes as well as transponder and biometrical locks
- Badge card systems with logging and alarm mechanisms
- CCTV monitoring
- Either manned reception or visitor policies, which requires accompanied attention
- Security guards
- Data centres are basically certified to ISO 27001

Control of Access to Data Processing Systems

Processor shall implement the following measures to prevent unauthorized access to data processing systems:

- Individual, identifiable and role-based allocation of USER Accounts
- Defined access privileges for user roles according to the “need-to-know” and “least- privilege-by-default” principles
- Role-based and password-protected access and authentication procedures
- In particular, passwords will be
- allocated uniquely,
- saved and transferred securely,
- defined as a complex string with a reasonable number of characters,
- changed regularly,
- limited in validity and blocked when not used temporarily and deleted when not used permanently,
- allocated manually and changed in the short term in case of an exposure to an unauthorized individual
- Automatic logoff in case of inactivity prompting for a new logon for further use of the system
- Deactivation of USER Accounts after three failed logon attempts
- All systems have centrally managed anti-virus and anti-spam programs

Control of Access to Data Applications

Processor shall implement the below listed measures to ensure that the data processing systems and applications can only be used by individuals authorized to access the data and only within the scope and to the extent required for the respective user role / access privilege and that personal data cannot be read, copied, modified or deleted without proper approval of the supervisor or his/her substitute

- Authentication at operating system level
- Separate authentication at application or “single-sign-on” environment level
- Authentication using a centrally managed authentication system (RACF, Active Directory, etc.)
- Division of responsibilities (technically / organizationally – double verification principle)
- Remote access only via VPN with the corresponding authorization and authentication
- Dedicated access control for all network systems and storage locations

Transfer Control

Processor shall implement the below listed measures to ensure that personal data cannot be read, copied, modified or deleted by unauthorized individuals during the transfer of data or during the transport of the data media and that it is possible to check and verify to whom personal data are transferred via networks.

- Firewall systems, proxy servers, NAT network compilation
- Possibility of email encryption and signature
- Data transfer control including encryption of data carriers / media
- Data transfer via secured data transfer protocols
- Encrypted VPN (virtual private network) with two-factor authentication
- Shipping of data tapes and other media exclusively by courier in secured containers, including documentation

Input Control

Regarding the User Administration the Processor shall implement the below listed measures to check and verify whether and by whom personal data have been entered into or deleted from the data processing systems.

- Documentation of administered activities (setup of USER Accounts, change management, access and authentication procedures, etc.)
- System log files activated by default with on-demand control
- Archiving of password resets and access requests (request / approval process)

The Controller is responsible regards the Input Control of contact data published within Material Data Sheets.

Order Control

Processor shall implement the below listed measures to ensure that personal data are exclusively processed according to agreement and Controller's instruction.

- Adherence to the obligations as defined in the Terms of Use, this Privacy Statement of DXC and, where appropriate EU standard contract provisions
- Control rights of Controller

Availability Control

Processor shall implement the below listed measures to ensure that personal data are protected from destruction or loss.

- Comprehensive and extensive data backup and recovery
- Disaster recovery and business continuity
- Storage and archiving policies
- Automatic anti-virus and anti-spam scans, including policies

Adequately equipped data centres, including physically separated backup data centres, if contractually agreed, as well as air conditioning and protection against other damaging environmental and sabotage impacts, including

- Uninterruptible power supply
- Redundant hardware and network systems, if contractually agreed
- Alarm and security systems (smoke, fire, water)

Separation Rule

Processor shall implement the below listed measures to ensure that personal data that are envisaged for different purposes can be processed separately.

- Data of different customers will be stored physically and/or logically separately (multi- customer systems)
- Access request and authentication processes ensure a separated processing of data of different customers or customer segments
- Separated test and production systems

(7) Rules for Correction, Deletion and Blocking of Data

Data processed under the Contract shall only be corrected, deleted or blocked by Processor in accordance with this Privacy Statement of DXC or Controller's instructions.

(8) Subcontracting

"Subcontracting" means third-party processing in terms of this Privacy Statement covering only services directly relating to the operation of the CDX platform. Ancillary services, such as operation and maintenance of the company-wide technical infrastructure, use of telecommunication services for company-wide communication and data management as well as services required in connection with the central customer / supplier management, are not in scope. The obligation of Processor to ensure compliance with data protection and data security regulations even in these cases, including Section V of the EU General Data Protection Regulation, remains unaffected.

The rules and obligations of Processor and Subcontractors set forth in this section apply mutatis mutandis to any Subcontractors commissioned by a Subcontractor.

Processor shall be liable for any non-compliance of a Subcontractor or its further Subcontractor with its data protection obligations.

Processor carefully selects the subcontractor, taking into particular consideration the technical and organizational measures taken by the subcontractor.

If data are not exclusively processed by subcontractors within the EU or the EEA, the provisions of Section (8), (9) and (10) of this Privacy Statement of DXC likewise apply to the subcontractor. A list of current subcontractors engaged by DXC for the provision of services shall be made available upon request to the Controller. Notwithstanding Controller's rights under applicable data protection laws, the continued use of the CDX service by Controller is deemed to constitute an affirmative action and therefore consent by the Controller to the Terms and Conditions as amended and communicated from time to time.

Processor shall regularly and reasonably monitor fulfilment of subcontractor's duties. The review and the result of the review shall be documented and made available to Controller upon request.

(9) Controller's Rights and Obligations

The responsibility for the assessment of the admissibility of commissioned processing and the protection of the rights of the individuals affected solely rests with Controller.

Controller shall immediately inform Processor about any errors or inconsistencies identified during the review of the results.

(10) Obligation to Provide Information

Processor shall comply with the legal provisions outlined in §§ 33, 34 GDPR.

(11) Inquiries regarding Data Privacy

In the case the USER has questions or concerns regarding his own specific personal data, USER can contact the CDX helpdesk:

CDX-ServiceDesk@dxc.com

(12) End of Contract / Data Retention

In the case a USER requests the termination of his own USER Account, Processor shall destroy or transfer the processed data on request and as selected by Controller, as far as no technical restriction of the CDX service applies (see above: last paragraph of Clause (2), (a.) “Subject Matter and Duration of Processing”).

Any existing copies of the personal data shall also be destroyed. The personal data shall be destroyed such that they or parts thereof cannot be restored at reasonable expenditure.

Processor shall initiate the immediate return or deletion of the personal data by subcontractors too.

Documentations supporting the proof of proper destruction shall be retained by Processor beyond the respective retention periods and thus also beyond the term of the Contract. To its discharge, Processor may provide such documentations to Controller at the end of the Contract.

(13) Miscellaneous

As far as this Privacy Statement of DXC does not stipulate a deviation the Terms of Use shall apply.

If individual parts of this Privacy Statement of DXC are invalid, the invalidity of such parts shall not affect the validity of the Privacy Statement of DXC as a whole.