

CDX Privacy Statement

Privacy Notice (Art. 13 GDPR)

CDX Controller

EntServ Deutschland GmbH, Schickardstrasse 32, 71034 Boeblingen, GERMANY

DXC Data Protection Officer

Mr. Carsten Weinholdt

Director, DXC Global Data Protection

DXC Technology Deutschland GmbH

CDX Contact: CDX-ServiceDesk@dxc.com

Legal Basis

DXC is processing personal data as a Controller (GDPR) on the following legal bases:

- **Consent** (Art. 6 para. 1 lit. a GDPR)
- **Performance of contract with a data subject** (Art. 6 para. 1 lit. b GDPR)
- **Legal obligation** (Art. 6 para. 1 lit. c GDPR)
- **Legitimate interest** (Art. 6 para 1 lit. f GDPR)

Data Subject Rights

As required by applicable laws, including GDPR where applicable, DXC provides you with reasonable access to personal data that you provided to CDX. We also give you a reasonable ability to review and correct your data or ask for deletion. To protect your privacy and security, we will take reasonable steps to verify your identity before proceeding your request. We may, for example, require a password and user ID to log into an application and/or other unique personal identifiers. To submit your access request, please email DXC Global Data Protection (GDP) Program at privacy@dxc.com and provide your legal name, relationship with DXC Technology, and country/state of residency.

Data subjects who are subject to GDPR shall have the following rights given to them under GDPR:

- Right of **access** (Art. 15 GDPR)
- Right to **rectification** (Art. 16 GDPR)
- Right to **erasure** (Art. 17 GDPR)

- Right to **restrict the processing** (Art. 18 GDPR)
- Right to **data portability** (Art. 20 GDPR)
- Right to **object** (Art. 21 GDPR)

Dispute or Complaint

The data subject can lodge a complaint with a supervisory authority, in particular in the EU/EEA Member State of residence if the data subject believes that DXC's processing of their personal data violates the GDPR or other data protection provisions. This right of appeal is without prejudice to any other administrative or judicial remedy.

Recipients

DXC may disclose personal data processed in CDX to the following categories of recipients:

- *DXC affiliates*
- *IT service providers or other service providers* (e.g. hosting or service providers for data center services or DXC's service providers for IT security or payment service providers)
- *Consultants and other persons who are bound by professional secrecy or confidentiality* (e.g. lawyers, tax consultants and auditors)
- *Government agencies and authorities* (only to the extent disclosure is necessary to fulfill a legal obligation)
- *Recipients during a reorganization, merger, divestiture or other transfer of assets*

To the extent that the recipients are data processors (under GDPR), they are subject to contractual obligations to process personal data only in accordance with DXC's written instructions and they are required to apply adequate measures to protect the confidentiality and security of personal data.

No obligation to provide personal data

Generally, Users are not obliged to provide DXC with their personal data to be processed in CDX. Registration is possible using generic business email address for instance. However, in this case only basic functions in CDX are available.

PRIVACY TERMS

1 Introduction, Scope, Definitions

This CDX Privacy Statement stipulates the rights and obligations of **Clients, Users** and EntServ Deutschland GmbH, Schickardstrasse 32, 71034 Boeblingen, GERMANY ("**DXC**") in connection with the processing of personal data as outlined in Regulation (EU) 2016/679 (General Data Protection Regulation – "**GDPR**").

"**Client**" means a company duly registered and authorized to use DXC's **Compliance Data Exchange System (CDX)**.

"**User**" means an authorized person accessing CDX.

A User represents and agrees on behalf of the Client or another legal entity to accept and abide by the **CDX Terms of Use** and this **CDX Privacy Statement**, when they create an account and use CDX.

Terms used in this CDX Privacy Statement which are not explicitly defined herein shall have the meaning given to them in the CDX Terms of Use or under the GDPR.

2 Roles and Responsibilities, Purposes and Duration of Data Processing

CDX processes personal data for the following purposes:

- (1) Client registration and User account creation, maintenance and deactivation
- (2) Provision of personal contact information in a Material Data Sheet

(1) Regarding Client registration and User account creation, DXC shall act as Controller (GDPR) because DXC determines the purposes and means of the processing. In this context, DXC shall be responsible for the proper collection, use, transfer, disclosure, retention and deletion of personal data.

(2) Regarding the provision and processing of personal contact information in a Material Data Sheet, Client, or the User representing the Client, shall act as Controller (GDPR) because they decide whether any contact information is added to a Material Data Sheet. If the Client or User decide to do so, it is upon them to determine what contact information is provided and whether it relates to an individual or is just generic. In this context, where the Client or User decide to provide individual contact information on a Material Data Sheet, the Client and User are responsible for compliance with laws applicable to the contact information about a living person ("**Contact Person**"). In particular, Client and User must rely on a proper legal basis when uploading personal contact information in a Material Data Sheet. Client and User are also responsible to manage any requests raised by a Contact Person when this person is exercising any rights given to it under applicable laws, including data subject rights under GDPR. If DXC is requested (by Client, User or a Contact Person) or legally forced (for instance by a supervisory authority, court order, or law enforcement) to delete personal information on a Material Data Sheet, the Client, and User representing the Client, hereby acknowledge

and agree to reimburse DXC for its efforts in doing so on a 'Time & Material' basis subject to the then current conditions.

DXC shall process Client and User personal data only as long as the registration is active. Upon request by the Client or User, or their self-deregistration, DXC shall deactivate the account. DXC shall continue to keep Client and User personal data secure for as long as legal retention times require and securely delete all personal data afterwards.

3 Categories of Personal Data, Data Subjects and Processing Activities

Client registration and User account creation, maintenance, and deactivation:

For each User (Client admin or Client user)

- Name (first name / last name)
- Email Address
- Phone Number
- Facsimile Number (optional)
- Title (optional)

Individual contact information provided in a Material Data Sheet:

- Personal contact details of a Contact Person including name and email address. A User has to identify itself as a "CDX contact" in his personal settings before it can be chosen by each User as a Contact Person for a material data sheet.

4 The Parties' Obligations

To the extent each party acts as an independent Controller, such party shall process personal data in accordance with its obligations under the GDPR. Such party shall in particular process personal data only to the extent required for the provision or use of CDX, and for the fulfillment of the CDX Terms of Use between the Parties.

DXC shall be responsible for the handling of data subject requests raised by a User, and the Client and/or User (as applicable) shall be responsible for the handling of data subject requests raised by a Contact Person. Taking into account the nature of the processing, each party shall assist the other party by appropriate technical and organisational measures, insofar as this is possible, for the fulfillment of the other party's obligation to respond to requests for exercising data subject's rights.

Unless otherwise stated in the CDX Terms of Use or this CDX Privacy Statement, any compensation and liability shall be handled in accordance with Art. 82 GDPR.

5 Transfer of Personal Data

Personal data submitted to CDX for User account creation and maintenance will be processed by DXC on IT-platforms operated within the European Union (EU) or within the European Economic Area (EEA) with support services, including remote services, from countries inside and outside the EU/EEA.

6 Personal Data Protection

DXC implements and maintains technical and organizational security measures (“**TOMs**”) to adequately protect the confidentiality, integrity and availability of the personal data processed in CDX, as well as adequate controls for Users to restrict and manage access to Material Data Sheets. The TOMs provided in **Annex 1** are subject to technological progress to ensure continued adequate level of protection.

7 Data Processors

DXC engages data processors in relation to the operation of CDX in accordance with the requirements under the GDPR for engaging data processors.

8 Inquiries regarding Data Privacy

USER: Questions from a User regarding its own personal data processed by DXC in CDX shall be directed to the CDX helpdesk at: CDX-ServiceDesk@dxc.com.

CONTACT PERSON: Questions from a Contact Person regarding its personal data mentioned in a Material Data Sheet shall be directed to the User who created and maintains the respective Material Data Sheet.

9 Data Retention

Upon the deletion of a User's CDX account, DXC shall remove and securely dispose of the User's personal data unless DXC is required to remain all or parts of User personal data for compliance with statutory legal and regulatory obligations. In this case, DXC shall apply proper data protection measures to the storage of the data during the legal retention period.

10 Miscellaneous

If any regulation of this Privacy Statement proves to be invalid or this Privacy Statement is incomplete, the remaining agreement shall continue in full force and effect. The parties shall replace such invalid regulation or any incompleteness of this Privacy Statement with a regulation which comes as close as possible to the economic intent of the original regulation.

This Privacy Statement shall be governed by German law. The courts of Frankfurt am Main, Germany shall have exclusive jurisdiction for any disputes arising from or in connection with this Privacy Statement. However, DXC may institute legal proceedings also in any other court having proper jurisdiction over the Client or User.

ANNEX 1 – Technical and organizational Measures (TOMs)

The following TOMs apply to DXC-owned and controlled devices used to operate CDX:

Control of Access to Processing Sites

DXC 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

- Badge card systems with logging and alarm mechanisms
- CCTV monitoring
- Either manned reception or visitor policies, which requires accompanied attention
- Security guards
- Datacenters are certified to ISO 27001

Control of Access to Data Processing Systems

DXC 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
- 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
- Locking 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

DXC 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

- Separate authentication at application or “single-sign-on” environment level
- Authentication using a centrally managed authentication system
- 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

DXC 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
- Email transport encryption
- 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

Input Control

Regarding the User Administration, DXC 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)

Order Control

DXC shall implement the below listed measures to ensure that personal data are exclusively processed according to the CDX Terms of Use.

- Consent: User must click OK on a statement and accept the CDX Terms of Use
- Adherence to the obligations as defined in the CDX Terms of Use and this CDX Privacy Statement

Availability Control

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

- Backup, disaster recovery and business continuity programs
- Storage and archiving procedures
- Anti-virus and anti-spam protection
- Datacenters, equipped with adequate protection against other damaging environmental and sabotage impacts, including
 - Uninterruptible power supply
 - Redundant hardware, network systems
 - Alarm and security systems (smoke, fire, water)

Separation Rule

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

- Data from different customers will be stored logically separately
- Access request and authentication processes ensure separation of personal data
- Test environment separated from production environment