# C:\Users\A3214804\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\QHB8Y02P\20140909 - Datenschutz -neu (2).pngTechnical and Organizational Privacy Measures

# Annex to CDP Agreement

Deutsche Telekom AG, Group Privacy

Version 1.0

Last revised 31 October 2017

Status final

public

Publication details

|  |  |  |
| --- | --- | --- |
| Published by | | |
| Group Privacy | | |
|  |  |  |
| File name | Document number | Document name |
| CDP annex TOM 1 v1-0 final eng.docx | v 1.0 | Annex TOM (IT-Configuration 1)  to CDP Agreement |
|  |  |  |
| Version | Last revised | Status |
| 1.0 | 31 October 2017 | Final |
|  |  |  |
| Author |  |  |
| Group Privacy |  |  |
| Bonn, October 2017 |  |  |
|  |  |  |
| Summary | | |
| This document is only valid as Annex to an Agreement on Commissioned Data Processing | | |
|  | | |

Contents

1. Admittance control 5

2. Access control 6

3. Data access control 8

4. Disclosure control 9

5. Processor control 12

6. Availability control 13

7. Intended use control 13

8. Organizational control 13

Preamble

The processor ensures,

* a specialist data privacy officer has been appointed in writing. His/her involvement in data privacy management is ensured,
* the organization must keep a directory of processing activities pursuant to Article 30 (2) GDPR. There is such a directory in written or electronic form. Or: This duty does not apply to the organization based on Article 30 (5) GDPR,
* that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality,
* when processing personal data, the implementation of any measures required to ensure an adequate level of protection pursuant to the requirements of Article 32 GDPR. Processing takes into account the status of the technology,
* the organization has an established process for giving notification of personal data breaches.

The processor uses for his services solely or additionally his own (or that of another processor) IT infrastructure (server/client, application) or his own end devices. He or third parties store personal data in his or third parties own responsibility respectively.

The processor fulfills the following mandatory marked requirements for the implementation of technical and organizational privacy measures.

1. Admittance control

The term “admittance” refers to the physical access by individuals to buildings and facilities in which IT systems are operated and used. These can be, for example, computer centers where web servers, application servers, databases, mainframes and storage systems are operated and office rooms where employees use desktop computers. This also includes the facilities where network components and network cables are located and laid.

100 Definition of security areas

The protection requirement of a building or a room is determined based on the data processing systems located in it with which the customer’s personal data is or can be accessed. The determining factor for the evaluation is the protection requirement of the customer’s data which the processor can access.

Fulfillment of the requirement 100 is a binding provision under this agreement.

101 Implementation of effective admittance protection procedures

Suitable technical measures (e.g., special glazing, intrusion detection system, chip-card operated turnstile, single-person security entry system, locking system) or organizational measures (e.g., security guard) shall be taken to safeguard security areas and their admittance points against entry by unauthorized persons.

Fulfillment of the requirement 101 is a binding provision under this agreement.

104 Specification of persons with admittance authorization

The requirements for and the group of persons with general admittance authorization must be defined and the authorizations for admittance to security-relevant areas limited to absolute necessity (“principle of minimal authorization”). Admittance shall be denied to anyone without authorization. Means of admittance to buildings or premises must only be issued to specific persons and may not be passed on to third parties. Users shall be made aware of this.

Fulfillment of the requirement 104 is a binding provision under this agreement.

105 Management and documentation of individual admittance authorizations throughout the entire life cycle

A process shall be established for requesting, approving, issuing, managing and accepting the return of means of admittance or for withdrawing admittance rights (including management of keys, visual IDs, transponders, chip cards, etc.); this process shall be described and implemented. Rules and procedures for blocking admittance authorizations shall be described. If an individual leaves the company or moves to a different department, all means of admittance and admittance authorizations for all premises that are no longer necessary for the performance of that person’s duties shall be immediately returned/revoked. All persons entrusted with security duties, in particular security gate duty, shall be notified of employees who have left the company or whose duties have changed.

Fulfillment of the requirement 105 is a binding provision under this agreement.

106 Accompanying visitors and external personnel

Written rules must exist governing the admittance of people external to the company, such as guests and suppliers. At the minimum, these rules shall require that people external to the company be able to prove at all times that they are authorized to be in the building, e.g., through a guest pass, visitor’s pass or supplier ID. The person’s name and origin (employer, business or home address) must be logged. A random check of authorizations to be in the building is obligatory. If there is a need for enhanced protection (protection class 3 or higher), non-company personnel shall be accompanied and supervised during the performance of their work.

Fulfillment of the requirement 106 is a binding provision under this agreement.

1. Access control

In addition to admittance control, the aim of access control is to prevent unauthorized persons from using data processing systems in which personal data is stored, processed or used.

202 Access protection (authentication)

Access to data processing systems on which data is processed should be possible only after the authorized person has been identified and successfully authenticated (e.g., with a user name and password or chip card/PIN), using state-of-the-art security measures. Access must be denied for lack of authorization.

Fulfillment of the requirement 202 is a binding provision under this agreement.

203 Strong authentication for maximum level of protection

Strong authentication is always based on multiple (at least two) factors, such as something owned, something known, or on the basis of a one-time factor that is specific to the user (usually biometric processes). Examples include:

* Chip card with certificates and PIN
* One-time passwords (OTP generator, SMS TAN, chip TAN) and user password
* Use of biometric procedures and password

Fulfillment of the requirement 203 is a binding provision under this agreement.

204 Simple authentication (with user name/password) for high level of protection

If the passwords are changed by the processor, they must obey appropriate minimum rules e.g., a minimum password length and complexity. Passwords have to be changed at regular intervals. Initial passwords must be changed immediately. The implementation of the requirements for password length, password complexity and validity shall be ensured by technical settings, if possible.

* A password consists of at least 8 characters.
* The password consists of a mix of characters. The available characters are divided into four categories:
* Lower-case letters, such as abcdefgh...
* Upper-case letters, such as ABCDEFGH...
* Numbers, such as 123456...
* Special characters, such as !“§$%...
* The mix of characters must consist of at least three of the categories shown above.
* Easy-to-guess words and trivial passwords may not be used for the password.
* A password shall be changed at regular intervals, but at least every year.
* When changing passwords, none of the last 4 passwords used may be reused
* The password shall not be visible in plain text on the screen when it is being entered.
* The initial password must be provided to the user through secure channels and/or the user must at least be prompted to change the password immediately after logging in for the first time.

Fulfillment of the requirement 204 is a binding provision under this agreement.

205 Logging access

All successful and rejected access attempts must be logged (user ID, computer, IP address used) and archived in an audit-compliant form for 3 months. To detect improper use, regular evaluations through sampling shall be carried out.

Fulfillment of the requirement 205 is a binding provision under this agreement.

206 Secure transmission of authentication credentials in the network

The authentication credentials (such as user ID and password) must never be transmitted unprotected over the network.

Fulfillment of the requirement 206 is a binding provision under this agreement.

207 Blocking passwords on failed attempts/inactivity and process for resetting blocked access IDs

Access must be blocked after repeated incorrect authentication attempts. A process shall be established for resetting or unlocking blocked access IDs; this process shall be described and implemented. User IDs that are not used for a long period of time (a maximum of 180 days) must be automatically blocked or set to inactive.

Fulfillment of the requirement 207 is a binding provision under this agreement.

209 Identification of authorized individuals

The group of people authorized to access IT systems of the customer must be limited to the absolute minimum necessary in order to perform the person’s specific duties or functions within the ongoing operational organization.

Fulfillment of the requirement 209 is a binding provision under this agreement.

210 Managing and documenting individual authentication media and access authorizations

A process shall be established for requesting, approving, issuing, and accepting the return of authentication media and access authorizations; this process shall be described and implemented. This includes at least a request and approval process as well as a process for accepting the return of authentication media and revoking access authorizations.

Access authorizations must always be assigned only for the data processing systems/types which need to be accessed for performing the person’s work (“principle of minimal authorization”). Authentication media and access IDs for accessing data processing systems shall, in principle, be assigned on an individual basis and be linked (user ID) to a personal credential (such as a password, token or chip card). Authentication media and/or user ID/password combinations must not be passed on to third parties. Users shall be made aware of this.

Rules and procedures for restricting processing or deleting them in compliance with data protection rules must be described. If an individual leaves the company or moves to a different department, all authentication media and access authorizations for all data processing systems that are no longer necessary for the performance of that person’s duties shall be immediately returned/revoked. Steps must be taken to ensure that all parties involved are notified of the fact that employees have left the company or changed jobs (in particular, IT/authorization administrators).

Fulfillment of the requirement 210 is a binding provision under this agreement.

214 Personal allocation of authentication media and access IDs

Authentication media and access IDs for access to installations and systems of the customer are always issued to a specific individual and linked to a personal password (user ID). Authentication media and/or user ID/password combinations must not be passed on to third parties.

Fulfillment of the requirement 214 is a binding provision under this agreement.

216 Conduct

The employee or vicarious agent of the processor/service provider must abide by the rules and guidelines of technical and organizational access control and must ensure that any access by unauthorized persons to the customer's IT systems due to misconduct on his/her part is prevented.

Fulfillment of the requirement 216 is a binding provision under this agreement.

1. Data access control

The data access control requirements are aimed at allowing only authorized persons to access the data which they are authorized to access and to prevent the data from being manipulated or read by unauthorized persons.

301 Creating an authorization concept

An authorization concept (user and administration rights) ensures that access to the data in the system is enabled only to the extent required for the user to complete the relevant task according to the user’s internal task distribution and separation of functions. Rules and procedures for creating, changing and deleting authorization profiles and user roles in compliance with data protection rules shall be described therein. The authorization concept must show which job holder may carry out administrative tasks (system, user, operation, transport) and which user groups may perform which activities in the system. Responsibilities are regulated.

Fulfillment of the requirement 301 is a binding provision under this agreement.

302 Implementing access restrictions

Each access authorization must be linked to a data access authorization, for example by linking it to one or more roles defined in the authorization concept. With the applications and within these applications, each access-authorized person may access only the data that he specifically needs to process the current transaction according to the order and which is configured in his individual authorization profile. To the extent that data of multiple customers is stored in the same database or is processed with the same data processing system, logical access restrictions must be provided which are aimed exclusively at processing the data for the customer concerned (multi-tenancy). The data processing function itself shall be limited to the extent that only the minimum functions needed can be used to process the personal data. Unique features are incorporated into the data processing systems which enable the accessing person to determine that the data processing system is authentic. The person authorized to access the data must also identify and authenticate himself to the data processing system on the basis of unique, verifiable factors, such as using ID reader on the terminals.

Fulfillment of the requirement 302 is a binding provision under this agreement.

303 Assigning minimum authorizations

The scope of the authorizations shall be limited to the minimum needed to perform the authorized person’s duties and functions. Time limits shall be put on access to personal data and authorizations to the extent possible that time limits can be put on certain functions without lowering the data processing quality.

Fulfillment of the requirement 303 is a binding provision under this agreement.

304 Managing and documenting individual data access authorizations

A process shall be established for requesting, approving, assigning, revoking and checking data access authorizations; this process shall be described and implemented. Rules and procedures for granting/revoking authorizations or assigning user roles shall be described. The data access rights must be implemented by the rights management process of the IT system.

Authorizations shall be linked to a personal user ID and an account. This excludes the use of group IDs/passwords used by multiple people.

When granting authorizations or assigning user roles, only the number of data access rights needed for performing the person’s duties shall be assigned (need-to-know- principle). Steps must be taken to ensure that the separation of functions mapped in the system is not canceled by cumulative authorizations.

If an individual leaves the company or moves to a different department, all data access rights for all data processing systems and data storage areas that are no longer necessary for the performance of that person’s duties shall be immediately revoked. Steps must be taken to ensure that all parties involved are notified of the fact that employees have left the company or changed jobs (in particular, IT/authorization administrators). The documentation shall be retained for 3 months.

Fulfillment of the requirement 304 is a binding provision under this agreement.

309 In-house maintenance, access to devices of the customer

If the processor performs the maintenance work at the customer’s premises or is given access to the customer’s hardware, the processor must ensure that he and his employees instructed with the work comply with the internal data protection and IT security rules and guidelines of the customer.

Fulfillment of the requirement 309 is a binding provision under this agreement.

1. Disclosure control

401 Determining instances/persons authorized to receive/transmit data

The processor and the customer must agree which bodies/persons are allowed to send which data to whom and the particular transmission path over which this may take place.

Fulfillment of the requirement 401 is a binding provision under this agreement.

402 Legality of transmission to other countries

In principle, it is possible to collect or process data in other countries only with the prior written approval of the customer.

Fulfillment of the requirement 402 is a binding provision under this agreement.

406 Transmission to external systems

If personal data is transmitted to external systems, encryption is absolutely necessary.

Fulfillment of the requirement 406 is a binding provision under this agreement.

408 Implementing security gateways at the network transfer points

The IT/NT systems on which personal data is processed shall be protected against unwanted access or data flows from both the same or other networks by using state-of-the-art measures (usually firewalls). Regardless of whether the firewalls are network/hardware-implemented or whether host-based firewalls are also used, the firewalls must be permanently activated. Steps must be taken to effectively prevent any form of deactivation or circumvention of the functions by the users. The rules must be set up in such a way that all but the necessary communications links are blocked automatically.

Fulfillment of the requirement 408 is a binding provision under this agreement.

409 Hardening the backend systems

The backend systems must be hardened according to state of the art technology to prevent attackers from gaining unauthorized access to the systems and data as a result of vulnerabilities.

Fulfillment of the requirement 409 is a binding provision under this agreement.

410 Describing all interfaces and the transmitted personal data fields

All interfaces to other IT processes shall be documented. This documentation must contain at least the following information:

* All personal data fields
* Direction of transmission (import/export)
* The respective purpose for the transmission
* The IT processes/interface to which the data is exported
* Type of authentication used by the interface
* Protection of the transmission (e.g., encryption)

In particular, the import and export interfaces from and to files must be described, along with how their use is protected through technical or organizational measures. Data migrations shall also be described accordingly as interfaces.

Fulfillment of the requirement 410 is a binding provision under this agreement.

412 Secure data storage

To securely store personal data with the highest level of protection, an encrypted data storage system shall be provided. This also applies to any backups.

Fulfillment of the requirement 412 is a binding provision under this agreement.

415 Secured storage on mobile data media

Storing data on mobile data media should be avoided due to the high risk of loss. However, if storing data on such media is unavoidable, the form of processing on this media shall be controlled and for the data stored thereon encryption shall be technically assured by default. Any data that is no longer needed must be immediately erased in compliance with data protection rules. The hardware used shall also be protected against loss/theft (by using cable locks, suitable lockable transport containers etc.).

Fulfillment of the requirement 415 is a binding provision under this agreement.

416 Introducing a process for managing data media

A qualified data media management system must exist. The data media management system must document how many data media containing personal data were created for which tasks and processing operations and where these media are stored up to the time they are destroyed. Regular inventory checks shall be carried out on the data media inventory. It is obligatory to store the created data media in a monitored security area if they contain personal data. The creation of data media copies must also be documented and retained for a period of 3 months after the assignment or activity has ended.

Fulfillment of the requirement 416 is a binding provision under this agreement.

419 Collection and disposal process

A process for collecting, disposing of, destroying or deleting non-electronic data media and information media must be established and described. Rules and procedures for the secure collection and internal forwarding as well as the storage and destruction of the media, taking into account the properties typical for the media, must be described in an organizational policy/process instruction. Destroying or erasing data media in compliance with data protection rules shall be carried out at the workstation in a timely fashion to largely avoid temporary media storage. This also limits the number of people handling the data media and increases security. Organizational steps shall be taken to rule out alternative disposal methods. Employees shall be made aware of this on a regular basis.

Fulfillment of the requirement 419 is a binding provision under this agreement.

420 Introduction of deletion and destruction methods in compliance with data protection regulations

For security reasons, unencrypted data media must be erased in compliance with data protection rules before being reused internally (e.g., changing primary user) or passed on to external parties. Formatting is unsuitable as a secure erasure method. Other secure erasure/destruction methods must be selected which make it extremely difficult to reconstruct the data.

Fulfillment of the requirement 420 is a binding provision under this agreement.

421 Maintaining erasure logs

The complete and permanent deletion of data and data carriers with personal data in compliance with data protection rules shall be logged. The logs shall be archived in an audit-compliant form for at least 12 months

Fulfillment of the requirement 421 is a binding provision under this agreement.

425 Passing on data media

For security reasons, unencrypted data must always be erased in compliance with data protection rules before being passed on to external bodies.

Fulfillment of the requirement 425 is a binding provision under this agreement.

426 Reproduction prohibition

Any kind of (electronic and/or analog) reproduction of data, data media or documents of the customer is not permitted unless it is an explicit part of performance of the assignment. If this is the case, copies must only be created for the purposes defined by the customer and only to the required extent. Electronic transmission via e-mail, for instance, is also a form of reproduction.

Fulfillment of the requirement 426 is a binding provision under this agreement.

427 Removable media

It is prohibited to connect external (removable) data media (USB, memory cards, CD/DVD, etc.) to data processing systems of the customer as well as to copy customer data to external (removable) data media, unless this is an explicit part of performance of the assignment and has been approved by the manager of the competent office of the customer.

Fulfillment of the requirement 427 is a binding provision under this agreement.

1. Processor control

603 Order execution rules and limitations

Only the work set forth in the service description to be prepared may be carried out. All activities that go beyond this scope must be discussed specifically in advance with the controller on the customer party and approved in writing. The processor must coordinate the scheduling of the work carried out on behalf of the customer with the customer in advance.

The processor must inform the customer without undue delay of any incidences of serious disruptions of operations, any suspicion of data protection violations, if errors or other irregularities occur in the handling of customer data. The processor must immediately remedy these problems.

At the end of the contractual relationship, the work results and the data, documents and operating supplies received must be handed over in the agreed manner.

Fulfillment of the requirement 603 is a binding provision under this agreement.

605 Other processors

To the extent the customer has approved the use of other processors (outsourcers/service providers - see definitions), the other processors must be carefully selected, the type and scope of the services to be provided arranged within the framework of a sub-contractual relationship which is in conformity with data protection law and the performance of activities and services must be checked in relation to the contractual regulations with the customer. The results of these checks must be documented in writing and presented to the processor on request. The customer’s direct right of control remains unaffected.

Fulfillment of the requirement 605 is a binding provision under this agreement.

606 Division of tasks

The division of tasks between the customer and the processor on the one hand and the processor and another processor on the other must be determined in writing before the activity is started if it does not result from the Agreements which have already been concluded.

Fulfillment of the requirement 606 is a binding provision under this agreement.

615 Handover at the end of the contractual relationship

At the end of the contractual relationship, the work results and the documents and operating supplies received must be handed over in the agreed manner.

Fulfillment of the requirement 615 is a binding provision under this agreement.

616 Configuration changes

Configuration changes to installations or systems of the customer are not permitted unless they have been explicitly agreed in writing as part of the assignment. If this is the case, the changes must be agreed in advance with the processing controller and their performance must be traceable in the form of appropriate documentation.

Fulfillment of the requirement 616 is a binding provision under this agreement.

1. Availability control

701 Backup concept

Data shall be backed up regularly in order to ensure that data is available even in an emergency. To achieve this, a backup concept shall be devised, which enables enable authorized employees to use all available means to restore data so that it can be made available again within a reasonable time after an incident.

Fulfillment of the requirement 701 is a binding provision under this agreement.

702 Emergency plan

The customer must be notified as quickly as possible of any disturbance (such as intentional internal or external attacks) or shutdown of the data processing work. If signs of a disturbance have been identified, immediate action must be taken to minimize damage and avoid any further damage. An emergency plan must be drawn up for this purpose, which lists the steps to be taken and determines the people, in particular those on the customer’s side, who need to be notified of the incident.

Fulfillment of the requirement 702 is a binding provision under this agreement.

1. Intended use control

801 Minimizing the amount of data collected

Only the amount of data that is essential to directly serve the actual purpose and perform the work or carry out the process shall be processed. This purpose may not change in any subsequent processing steps, including after transmission.

Fulfillment of the requirement 801 is a binding provision under this agreement.

802 Separate processing

Rules and measures to ensure that data and/or data media used for different contractual purposes are processed and/or stored separately shall be documented and applied.

Fulfillment of the requirement 802 is a binding provision under this agreement.

1. Organizational control

902 b Implementation of training measures

All individual who deal with personal data or who are otherwise involved in order processing (such as maintenance companies or data destruction companies, where agreed) must be verifiably instructed in the following areas:

* The principles of data protection, including technical and organizational measures
* The requirement to maintain data secrecy and confidentiality about company and trade secrets, including customer transactions
* The proper, careful use of data, data media and other documents
* Telecommunications secrecy (requirement defined in Article 88 TKG)
* Other specific confidentiality obligations, where necessary
* Other specific information that can result from the contractual agreement and from this catalog of minimum requirements, where necessary.

The instruction must take place through suitable measures that are appropriate to the order, and it must be repeated at least every two years, or even at shorter intervals, if needed (e.g., if the circumstances of the order or legal provisions change).

Fulfillment of the requirement 902 b is a binding provision under this agreement.

905 Separation and assignment of functions

A separation of functions must be defined, documented and explained, i.e., which functions cannot be combined with each other, and thus may not be performed by the same person at the same time. Requirements for this can result from the task itself, the requirements of this agreement, (especially the list of minimum requirements and supplementary standards) or from legal regulations. In principle, operational functions cannot be combined with controlling functions. After the separation of functions to be observed has been defined, the functions must be assigned to people.

Fulfillment of the requirement 905 is a binding provision under this agreement.

908 b Internal audits

All read, input, modification and deletion transactions must be logged (user ID, transaction details).

Internal audits on the processor’s premises ensure that the logs showing access to the personal data are analyzed regularly, but at least every 2 months. Irregularities are documented, communicated to the customer immediately in writing and retained for a period of 3 months after completing the order or the activity.

Fulfillment of the requirement 908 b is a binding provision under this agreement.