Technical and organizational Data Privacy measures
Appendix to the Commissioned Data Processing Agreement (CDPA) - Scenario 2

Deutsche Telekom AG

Version	3.0
Last revised	01.12.2021
Status	final

public

Publication details

Published by

Deutsche Telekom AG
Group Privacy

File name	Document number	Document name
CDPA Appendix TOM S2 v03 final.docx	v 3.0	Technical and organizational Data Privacy measures Appendix to the Commissioned Data Processing Agreement (CDPA) - Scenario 2-

Version	Last revised	Status
3.0	01.12.2021	final

Author

Group Privacy
Bonn, December 2021

Brief info

This document is only valid as an Appendix to a Commissioned Data Processing Agreement

Contents

1. Introduction

The technical and organizational measures (TOM) defined in this document supplement the provisions set down in the Framework Agreement (in order to implement the requirements defined in Article 32 of the GDPR). The provisions of the Framework Agreement apply in full to commissioned data processing. The requirements defined in this Appendix apply in addition, depending on the specified scenario. A general distinction is made between the following scenarios in the Appendices to the Framework Agreement:

- Scenario 1: The processor solely or additionally uses its own IT infrastructure (server/client, application) (or the IT infrastructure of a subcontractor) or its own devices. Or: The processor or a person commissioned by the processor stores the controller's personal data in the processor's/commissioned person's own IT infrastructure or devices.
- Scenario 2: The processor uses the controller's IT infrastructure (server/client, application) and accesses the latter using its own devices (or those of a subcontractor). No data are stored at the processor or a third party.
- Scenario 3: The processor exclusively uses the responsible Customer's IT infrastructure (server/client, application) and devices.

This Appendix to the Commissioned Data Processing Framework Agreement (CDPA) and Overall Commissioned Data Processing Agreement (CDPA) refers to scenario 2 with the following conditions:

- The processor uses the controller's IT infrastructure (server/client, application) and accesses the latter using its own devices (or those of a subcontractor).

- No data are stored at the processor or a third party.

- In addition, the processor meets Deutsche Telekom's requirements (specified as binding below) for implementing the technical and organizational measures.

1.1 User instructions

The measures defined in section 2 implement the requirements of Art. 32 GDPR and its protection targets in concrete terms. The setup of the targets depends on both the type, volume, and form of data to be processed as well as on the local circumstances in question. Depending on the type of commissioned data processing further requirements may arise. These could be sector-specific (e.g. health care, banking sector), country-specific (e.g. country specific laws) or additional Telekom group specific requirements.
The following section classifies the corresponding measures for each data protection goal.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

1.2 Definition of terms

A distinction is made between standard and high protection levels in the requirement definitions for the technical and organizational measures. A high protection level is required if:

- the personal data being processed come under the special categories specified in Article 9(1) GDPR
- the form of processing meets the criteria which require a data protection impact assessment to be carried out in accordance with Art. 35 DSGVO, e.g. at least in one of the following cases:
    - systematic monitoring / scoring / profiling,

- Data transfer to countries outside the EU/EEA,
- Traffic data of telecommunications / usage data of tele media,
- Localization data,
- Targeted performance and behaviour monitoring of employees,
- Account data of persons, identity card / passport,
- Contract data, such as customer number, date of birth,
- Sensitive data of employees, such as criminal record, pension data, personnel number, time recording,
- Extensive data records, e.g. for private address/telephone number.

If personal data require different protection levels, i.e., individual elements belong to different protection categories, the highest protection category applies. The protective measures to be taken reflect this.

2. Technical and organizational measures

Data protection goal 1 – Availability

The "Availability" data protection goal refers to the requirement that personal data can be accessed and processed promptly, and that they can be used properly in the designated process. For this purpose, they must be accessible to authorized persons and the designated methods for their processing must be able to be applied to them.

Req 1.1 Physical protection from external threats

Measures to protect against internal and external threats are formulated and implemented at the processor. These are used as protection:

- From natural disasters, attacks, or accidents,
- From incidents such as power failures or other supply issues,
- For the cabling from interruption, incident, or damage.

The effectiveness of the physical protection measures must be tested on a regular basis. The protection concept must also be adapted in the event of changes to the processing of data. Corresponding processes must be implemented by the processor.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 1.2 Protection of the IT systems and networks from external threats

The processor has defined and implemented regulations that protect the IT systems, networks, and components (technical equipment, utilities, etc.) that are used for processing personal data from unauthorized access, unauthorized modification, loss or destruction, or false or unlawful use. These regulations apply over their entire lifecycle.
Furthermore, data protection and security are integrated into business continuity management such that processes, procedures, and measures ensure commissioned data processing is contractually compliant even in adverse situations. The processor regularly reviews their effectiveness and ensures availability, e.g., through redundancies.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 1.3 System hardening

Information and information-processing equipment are protected against malware and information-processing systems are hardened. Suitable software (e.g., virus scanners, IDS) are installed and kept up-to-date to protect the systems. When a system is hardened, the following points must be taken into account as a minimum:

- The patch level is up-to-date.
- System installation often involves installing software components or even activating individual software parts that are not required for the system's subsequent operation and functionality. Such

components were either not included during installation, or else they were removed afterwards. Furthermore, no software was installed in the systems that is not necessary for the system's subsequent operation, maintenance, or functionality.
- In addition to software functions, no hardware functions that are not required for the system's operation are activated after the system installation, either. Functions such as interfaces that are not required are permanently deactivated, ensuring that they remain deactivated even when the system is restarted.
- All unnecessary services in a system and in the interfaces were completely deactivated and remain deactivated even when the system is restarted.
- The accessibility of a service via the necessary interfaces was also restricted to legitimate communication partners.
- Preconfigured service accounts that are not required were deleted and default passwords were changed.
- It is common practice for manufacturers, developers, or suppliers to preconfigure authentication features such as passwords and cryptographic keys in systems. Such authentication features were changed to separate features that third parties are not aware of.
- If the system is operated on a cloud platform, this prevents the system (or the entire client/tenant with all of its services and data) from being deleted accidentally or by unauthorized persons.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 1.4 Backup concept

The processor has defined and applied regulations that ensure a suitable backup strategy is in place. This particularly takes into account requirements regarding system availability, regular testing of recoverability, and legal requirements concerning storage or deletion.
The objective of this measure is to ensure that the live data are mapped consistently in the event of an emergency. Depending on the framework conditions, different strategies can be used here. In addition to a classic backup solution, it is also possible to operate mirroring systems in a different security area, or even a combination of both strategies.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 1.5 Personnel concept for ensuring the protection goals

The processor has implemented a personnel concept that supports data protection by means of the following measures:
- Only expert staff are used who can demonstrate that they have attended all necessary training and obligations to maintain confidentiality and observe telecommunications secrecy.
- A responsible contact is defined for all processing of personal data. A deputization arrangement is in place.

When their employment relationship, contract, or agreement ends, employees and processors return the assets that they were given to perform their task to the organization (controller/processor). These include means of access, computers, storage media, and mobile devices.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 1.6 Creation of an emergency concept to restore a processing activity

The processor has implemented an emergency concept to restore data processing. The objective of this concept is to restore availability following a processing incident. The emergency concept must satisfy the following requirements/criteria:

- There are rules that define the time needed to restore regulated data processing following an incident.
- Resources are provided to restore the data
- Responsibilities have been assigned
- Verified measures for defending against the incident and restoring regular operation have been defined
- Information and escalation chains exist
- The interactions with corresponding processes and rules (backup concept, personnel concept, etc.) have been defined

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Data protection goal 2 – Integrity

On the one hand, the "Integrity" data protection goal indicates the requirement for IT processes and systems to comply continuously with the specifications that were defined for them, so they can execute their intended functions. On the other, "Integrity" refers to the property whereby the data to be processed remain intact, complete, correct, and up-to-date.

Req 2.1 Definition, use, and monitoring of the target behavior of processes

The processor has established binding processes on implementing data protection and information security by the management or executive board. These are fixed in writing, freely accessible, disclosed to all internal and external employees, and applied. The objective of these specifications is to implement the processing of personal data in such a way that the defined target behavior of the processes is guaranteed at all times. The provisions are reviewed regularly to ensure they are effective, up-to-date, and compliant with regulations.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 2.2 Authorization concept

The processor uses up-to-date authorization concepts that specify bindingly who can access which systems, databases, or networks, and when. This authorization concept must satisfy the following properties:

- Defined authorizations exist in the form of roles based on business, security-relevant, and data protection requirements.
- The roles are documented and up-to-date.
- Roles are uniquely assigned to users or machines.
- Users have exclusive access to the networks, systems, and data for which they are explicitly authorized.
- A formal process for registering and deregistering has been implemented so that access rights can be assigned.
- A formal process for granting user accesses has been implemented to assign or withdraw access rights for all user types to all systems and services.
- The allocation and use of privileged access rights are restricted and monitored continuously.
- The allocation of access rights is monitored with the objective of preventing rights from being allocated across functions.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 2.3 Identity management

Authorization for access to personal data is not allocated until after the user has been uniquely identified. Users can be identified uniquely by a system. To achieve this, an individual user account is used for each user. Group accounts, where one user account is used for several people, are not used.
One exception to this requirement are machine accounts. These are used for authenticating and authorizing systems among each other or by applications in a system, which means that they cannot be assigned to a single person only. Such user accounts are assigned individually per system or per application. This ensures that such user accounts cannot be misused.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 2.4 Crypto concept

The processor has defined and implemented the use of cryptographic measures to protect personal data through a guideline. This guideline regulates and guarantees:

- The use of state-of-the-art cryptographic procedures
- The required protection level of the personal data based on a risk assessment
- The management and use of cryptographic keys
- The protection of cryptographic keys throughout their life cycle (creation, storage, application, and destruction).

The objective of such a crypto concept is:

- To ensure the integrity of sensitive data
- To secure identity management processes
- To support authorization processes
- To ensure the confidentiality and integrity of sensitive data

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Data protection goal 3 – Confidentiality

The "Confidentiality" data protection goal refers to the requirement that no unauthorized person can access or use personal data. Unauthorized persons are not only third parties external to the controller, but also employees of technical service providers who do not need access to personal data as part of the provision of service, or persons in organizational units who do not have any content-related reference to a processing activity, or to the relevant data subject.

Req 3.1 Definition and monitoring of the use of permitted resources and communications channels

With the following measures, the processor ensures that the resources and communications channels that are used for processing personal data are defined, and that their use is monitored:

- Areas are defined depending on the protection level; the required security perimeters are specified and implemented. The protection level is classified based on the personal data or information-processing systems located in the areas (including mobile workstations).
- Suitable admission control rules are defined and applied that ensure only authorized persons gain access to the defined areas.
- A system access control guideline is to be created and implemented at the organization based on data protection regulations and security requirements. This guideline is to regulate access to personal data depending on the required protection level and on a need-to-know basis. This particularly includes access to IT systems, networks, and databases containing personal data.
- Rules exist for transporting data carriers in accordance with the protection level required for the personal data. If personal data are not encrypted, appropriate alternative protective measures must be taken. If a high level of protection is needed, there are special requirements concerning the reliability of transport, the obligation to encrypt data, and obligations relating to documentation, logging, and provision of evidence.
- Guidelines, security procedures, and control measures exist to protect the transmission of information for all types of communication equipment (including mobile workstations). When personal data are transmitted over public networks, they are always encrypted.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 3.2 Secure authentication procedures

Systems and applications are accessed by means of a secure authentication procedure. The authentication procedure must be appropriate for the protection level applicable to the personal data that can be accessed after authentication was successful. If the protection level is high, login procedures that are based on possession and knowledge (two-factor authentication) must be used. A high protection level is to be assumed if access to data is enabled that falls within Art. 9 (1) GDPR. If the protection level is low, authentication using a username and password is sufficient. In general, the selected authentication procedure satisfies the following criteria:

- All user accounts in the system are protected from use by unauthorized persons. For this purpose, the user account is secured with an authentication feature that enables the accessing user to be uniquely authenticated. Authentication features include passwords, passphrases, PINs, (factor

knowledge)/cryptographic keys, tokens, smartcards, OTP (owner)/or biometric features such as fingerprints or hand geometry (inherence)
- The specifications for creating passwords (length, complexity, reuse, etc.) are governed at least by cutting-edge technology
- When passwords are used as the authentication feature, protection exists against online attacks such as dictionary and brute force attacks
- The system provides functions that enable users to change their password at any time.
- Passwords are saved using a cutting-edge, cryptographic one-way function that is appropriate for this purpose and has been classified as secure (called "password hashing")
- Any systems used for managing and allocating passwords ensure that strong passwords are set up. If access takes place automatically, through auxiliary programs, or through routines in software development, usage is kept to a minimum and the application is monitored regularly.
- Users with extended authorizations within a system, such as access to highly sensitive personal data, configuration settings, or administration accesses, are given at least two authentication features that are independent of each other to achieve an appropriate level of protection. The authentication features that are used must consist of different factors (knowledge, ownership, inherence). This approach is generally known as MFA (multi-factor authentication). A specific type of MFA is 2FA (2-factor authentication), which combines exactly two authentication features. A combination of authentication features of the same factor (such as two different passwords) is not allowed.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Data protection goal 4 – Unlinkability

The "Unlinkability" data protection goal refers to the requirement that personal data must not be merged, i.e., chained. It must be implemented in particular when data to be merged were collected for different purposes. The larger and more meaningful data records are, the greater the desire may be to use the data outside of their original legal basis.

Req 4.1 Definition and determination of the processing purpose

Using appropriate measures, the processor ensures that the personal data processed are processed only in the context of the contractually agreed purpose. These measures include:
- Internal documentation and communication of the intended purpose in all data processing procedures
- Regulated change of purpose procedures

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 4.2 Measures for ensuring purpose limitation

The processor ensures that personal data are processed exclusively for the contractually agreed purpose, and that only persons/instances authorized to process the data have access to them. In addition to the defined requirements for the data protection goals of availability, integrity, and confidentiality, the following measures were taken to avoid chaining data records with different purpose limitations:

- Restriction of processing, usage, and transmission rights to the extent that is absolutely necessary for processing
- Separation by organizational/departmental boundaries
- Separation of environments by role concepts with tiered access rights on the basis of identity management and by means of secure authentication procedures
- Development, test, and operating environments must be logically separated at least. Suitable access controls were implemented to ensure that access is restricted to properly authorized individuals. Within these environments, the processing of personal data was separated from other types of data. This separation was implemented either physically or logically.
- If test or development networks or devices require access to the operating network, strict access controls were implemented.
- Personal data cannot be processed in test and development environments. Exceptions to this rule must be defined by separate, written instructions from the customer.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Data protection goal 5 – Transparency

The "Transparency" data protection goal refers to the requirement that to differing degrees, both data subjects and the operators of systems, as well as responsible control instances, can identify which data is collected and processed when and for what purpose during a processing activity, which systems and processes are used for this, where the data flows for which purpose, and who has legal responsibility for the data and systems in the different data processing phases.

Req 5.1 Documentation of the data processing

The processor documents the processing of personal data as follows:

- The processing process is documented in such a way that it is fully transparent how the processing of personal data is implemented. This relates to the entire processing cycle, from the acceptance/creation of personal data to their forwarding/deletion.
- Incidents, processing problems, and changes to processing activities or the technical and organizational measures are all documented
- It is also documented who has access to the data and at what time.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 5.2 Documentation and storage of contracts, agreements, and instructions

The processor stores all contracts, agreements, or instructions securely. This means that they are available at all times to the contracting parties or supervisory authorities.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 5.3 Logging of the data processing

Access by users and system administrators to personal data must be logged and regularly checked, taking the principle of data minimization and the protection level into account. The access and the type of access (e.g., read, edit, delete) is logged.
Relevant events, exceptions, incidents, and information security incidents are logged and checked regularly.
The logs are stored such that they cannot be accessed by the logged system administrators or users.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Data protection goal 6 – Intervenability

The "Intervenability" data protection goal refers to the requirement that the data subject is immediately and effectively entitled to their rights to notification, information, rectification, deletion, restriction, data portability, objection, and intervention in automated individual decisions if the legal requirements exist, and the processing department is obliged implement the corresponding measures.

Req 6.1 Implementation of measures for implementing data subject rights in the system design (privacy by design)

The processor implements the data subject rights and data protection requirements during the system design. The following measures must be implemented during the system design (processes and software):

- Definition of default settings for data subjects that restrict the processing of their data to the extent required for the purpose of the processing.
- Provision of options for data subjects so that programs can be configured to comply with data protection requirements
- Deactivation option for individual functions without affecting the system as a whole.
- Implementation of standardized query and dialog interfaces for data subjects to assert and/or implement demands
- Operation of an interface for structured, machine-readable data that can be called by data subjects
- Reduction in the processing options in processing steps
- Creation of the required data fields e.g., for lock indicators, notifications, consents, contradictions, counterstatements
- Removal of data fields and options that are not necessary, reduction in output following search requests in databases, minimization of export and print functions

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Data protection goal 7 – Data minimization

The "Data minimization" data protection goal comprises the fundamental data protection guideline of restricting the processing of personal data to the extent that is appropriate, significant, and necessary for the purpose. This obligation of minimization has a drastic influence on the scope and intensity of the protection program that is determined by the other data protection goals.

Req 7.1 Operational measures for minimizing data

The processor takes operational measures with the objective of restricting the processing of personal data for a specific purpose to a minimum. The following measures have to be implemented:

- The attributes that are recorded relating to the data subject are restricted to the necessary minimum
- When personal data are forwarded, only those attributes are forwarded that are essential for the purpose of the processing of the subsequent process step.

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*

Req 7.2 Technical measures for minimizing data

The processor takes technical measures with the objective of restricting the processing of personal data for a specific purpose to a minimum. The following measures are suitable:

- Restriction of the processing options in processing steps
- Implementing data masks that suppress data fields, as well as automatic lock and deletion routines, use of pseudonymization and anonymization procedures
- Restrictions of the options of accessing available data (display options, search fields, etc.) to the absolute minimum

If a measure cannot be implemented or can only be partially implemented, a justification and the indication of alternative measures ***must be provided in the TOMs of the individual CDPA corresponding to the intended purpose of use*** *(to be completed during the order process).*