Technical and organizational Data Privacy measures
Appendix to Commissioned Data Privacy Agreement (CDPA) - Scenario 3

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 S3 v03 final.docx	v 3.0	Technical and organizational Data Privacy measures Appendix to the Commissioned Data Processing Agreement (CDPA) - Scenario 3-
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 3 with the following conditions:

- The processor only uses the IT infrastructure (server/client, application) and end devices of the responsible party.

- No data is stored by the processor or a third party.

- In addition, the processor fulfills the following Deutsche Telekom requirements, which are marked as mandatory, for the implementation of 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,
- o 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 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).*

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 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 2.2 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).*

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.

In the present scenario, the measures to ensure confidentiality are ensured by the responsible body (controller).

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.

In the present scenario, the measures to ensure unlinkability are ensured by the responsible body (controller).

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.

In the present scenario, the measures to ensure data minimization are ensured by the responsible body (controller).