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

Deutsche Telekom AG

<table>
<thead>
<tr>
<th>Version</th>
<th>2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last revised</td>
<td>01.06.2020</td>
</tr>
<tr>
<td>Status</td>
<td>final</td>
</tr>
</tbody>
</table>

public
### Publication details

**Published by**
Deutsche Telekom AG  
Group Privacy

<table>
<thead>
<tr>
<th>File name</th>
<th>Document number</th>
<th>Document name</th>
</tr>
</thead>
</table>
| CDPA Appendix TOM S3 v02 final EN.docx | v 2.0 | Technical and organizational Data Privacy measures  
Appendix to the Commissioned Data Processing Agreement (CDPA) - Scenario 3- |

<table>
<thead>
<tr>
<th>Version</th>
<th>Last revised</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>01.06.2020</td>
<td>final</td>
</tr>
</tbody>
</table>

**Author**

Group Privacy  
Bonn, September 2019

**Brief info**

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

1. Introduction ..................................................................................................................................................... 4  
   1.1 User instructions............................................................................................................................................. 4  
   1.2 Definition of terms .......................................................................................................................................... 5  
2. Technical and organizational measures .................................................................................................... 6
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. When interpreting the requirements, the specifications in ISO/IEC 27001:2017-06, ISO/IEC 27002:2017-06, ISO/IEC 27701:2019(E), and ISO/IEC 29151:2017 (E) must be taken into account; this also applies to matters that are not covered by the requirements. 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.

Relevant references to the GDPR and the respective ISO standards are attached to each of the measures below.
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

01 Regulations and measures on the use of information and assets that enable processing of personal data

The organization has defined and implemented regulations that protect information and assets (data, technical equipment, utilities, etc.) that are used for processing personal data from unauthorized access, unauthorized modification, loss or deletion or false or unlawful processing. These regulations apply over the entire lifecycle of information and assets.

References

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Article 32(1a-c) and Article 6(4) (confidentiality, availability, integrity, pseudonymization, encryption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001:2017-06</td>
<td>Table A1: A.8.1.3</td>
</tr>
<tr>
<td>ISO/IEC 29151:2017 (E)</td>
<td>8.1.4</td>
</tr>
</tbody>
</table>

02 Returning assets

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

References

<table>
<thead>
<tr>
<th>GDPR</th>
<th>Article 32(1b) and Article 28(3g) (confidentiality, integrity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001:2017-06</td>
<td>Table A1: A.8.1.4</td>
</tr>
<tr>
<td>ISO/IEC 29151:2017 (E)</td>
<td>8.1.5</td>
</tr>
</tbody>
</table>