Supplementary Terms and Conditions for Data Processing (STC-DP) for Open Telekom Cloud

The contractual partners are T-Systems International GmbH (hereinafter referred to as Telekom), Hahnstrasse 43d, 60528 Frankfurt am Main, Germany and the customer.

1 General

The subject matter of the agreement is the regulation of the rights and obligations of the customer (hereinafter also referred to as the controller) and Telekom (hereinafter also referred to as the processor), to the extent that the processing of personal data as part of the service provision (in accordance with the General Terms & Conditions and other applicable Telekom documents) is carried out by Telekom for the customer within the meaning of the applicable data protection laws. For the avoidance of doubt, although the customer is referred to as controller in this agreement customer can either act as controller or processor of data processed by customer on behalf of its customer. In this case Telekom will act as a subprocessor of customer.

This agreement is intended to provide compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679 (GDPR).

The subject matter and duration as well as the type and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller and processor result from the General Terms & Conditions, the other applicable documents, these "Supplementary Terms and Conditions for Data Processing" and the related annexes ("STC-DP").

For this purpose, the parties agree to the standard contractual clauses published by the European Commission (EU Commission) pursuant to Article 28 (7) of the GDPR in accordance with Implementation Decision (EU) 2021/915 of June 4, 2021, (hereinafter referred to as the "clauses"). These clauses are listed in cipher 2 with the respective selected option in the original text.

Further provisions within the meaning of clause 2 letter b are agreed by the parties in cipher 3, 4, and 5 of this STC-DP. The regulations take particular account of the fact that Telekom's service is a standardized General Terms & Conditions product. The parties agree that these provisions do not conflict with the clauses.

2 Standard contractual clauses ("clauses")

SECTION I

Clause 1 [Purpose and scope]

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [OPTION 1:]

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2 [Invariability of the Clauses]

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3 [Interpretation]

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4 [Hierarchy]

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 [Docking clause]

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

Obligations of the parties

Clause 6 [Description of processing]

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 [Obligations of the parties]

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of subcontracted processors

(a) GENERAL WRITTEN AUTHORIZATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least four weeks in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object. [OPTION 2]

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any

failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8 [Assistance to the controller]

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679. [OPTION 1]

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9 [Notification of personal data breach]

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679 [OPTION 1], shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 [OPTION 1], with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679. [OPTION 1]

SECTION III

FINAL PROVISIONS

Clause 10 [Non-compliance with the Clauses and termination]

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

3 Other clauses within the meaning of clause 2 b

3.1 [Instructions]

The parties agree that instructions within the meaning of clauses 7.1 letter a and 7.2 shall initially be understood to mean the General Terms & Conditions, other applicable documents and these STC-DP. Furthermore, within the scope of the product-specific parameters, the controller may determine the type and scope of data processing by the way the product is used and by selecting any possible variants. Instructions of the controller can be made within the agreed scope of the standard product. In the event of further instructions from the controller that go beyond the agreed scope, cipher 4 of this STC-DP (Amendments) shall apply.

3.2 [Additions to clause 7.6]

With regard to clause 7.6, the parties agree that the controller shall use suitable certifications from and other documents submitted by as a matter of priority to prove compliance with the clauses as well as with the obligations set forth in these clauses and arising directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. In addition, it may carry out an on-site inspection in exceptional cases that require special justification.

3.3 [Changes by the customer]

The list of sub-processors approved by the Controller (GENERAL WRITTEN APPROVAL pursuant to Clause 7.7(a)) can be found in Annex IV. The Processor shall inform the Controller in text form six weeks in advance of any planned changes to sub-processors who process the Customer's data on behalf of the Processor and shall provide the Controller with the information required to exercise its right of objection. The Controller shall notify the Processor in writing within two weeks whether it objects to this change. If the Controller does not object within two weeks of notification of the change, the change shall be deemed approved. The Controller shall not object unreasonably. If the Controller raises an objection and the Processor's performance becomes impossible as a result, the Controller may terminate the affected services without notice.

3.4 [International data transfer]

Section 7.8 is replaced by:

There shall be no transfer of data by the Processor to a third country without an adequacy decision by the EU Commission pursuant to Article 45 of the GDPR.

3.5 [term assignment]

The parties agree that the terms "shall ensure" and "ensure", insofar as they are used in the clauses, do not constitute a guarantee in the legal meaning.

3.6 [Addition to clause 10 d) and Art. 28 para. 3 g) GDPR]

The parties agree that clause 10 letter d and Art. 28 (3 g) of the GDPR shall be interpreted in such a way that there is a right to choose between erasure and return only if the agreed service allows both options.

4 Miscellaneous

4.1 [Customer's area of responsibility]

The customer is responsible for assessing the permissibility of data processing. The customer shall ensure in its area of responsibility that the necessary legal requirements are met (e.g., by collecting declarations of consent) so that Telekom can provide the agreed services in a way that does not violate any legal regulations.

4.2 [Validity of the agreement]

The invalidity of a provision of this STC-DP shall not affect the validity of the remaining provisions. If a provision proves to be invalid, the parties shall replace it with a new provision which approximates to the intentions of the parties as closely as possible.

4.3 [Place of jurisdiction]

For disputes in connection with this STC-DP, the place of jurisdiction is that which has been agreed in the General Terms & Conditions. If the General Terms & Conditions do not contain such an agreement, the sole place of jurisdiction shall be Bonn. This shall apply subject to any sole statutory place of jurisdiction.

4.4 [Priority regulation]

In the event of contradictions between the provisions of this STC-DP agreement and the provisions of other agreements, in particular the General Terms & Conditions and the other applicable documents, the provisions of this STC-DP agreement shall prevail. In all other respects the provisions of the General Terms & Conditions and the other applicable documents shall remain unaffected and shall apply to this STC-DP agreement accordingly.

Annex I Supplementary Terms and Conditions for Data Processing (STC-DP) for Open Telekom Cloud

List of parties

The parties to the agreement are the contractual partners of the Service Agreement.

Annex II Supplementary Terms and Conditions for Data Processing (STC-DP) for Open Telekom Cloud

Description of the processing

1 Details about the data processing

a. Type of service

☒ IaaS (Infrastructure as a Service)
☒ PaaS (Platform as a Service)
☒ SaaS (Software as a Service)

b. Categories of data subjects

☒ Customers of the Controller
☒ Employees of the Controller
☒ Personal data of persons processed by the customer in the Open Telekom Cloud

c. Category of personal data:

☒ Master data of the controller's customers
☒ Contact data of the controller's customers
☒ Personal data for logging (e.g. user ID, IP address)
☒ All other personal data defined in Art. 4 No. 1 of the GDPR that is transmitted or stored by the customer in the course of using the product and to which access by Telekom's system administrators cannot be completely ruled out.

d. Sensitive personal data

Sensitive personal data and applied restrictions or safeguards (Art. 9 GDPR, Art.10 GDPR) that take full account of the sensitivity of the data and the associated risks (e.g. additional security measures):

None.

2 Access to personal data

The customer shall provide Telekom with the personal data, enable Telekom to access the personal data, or allow Telekom to collect the personal data by transmitting this data to Telekom via a secure internet connection. As a rule, Telekom does not have access to the customer's personal data. However, this cannot be completely ruled out in exceptional cases, e.g., maintenance
or troubleshooting cannot be completely ruled out and only takes place with the customer's only after separate approval by the customer.

3 Services; purpose of the agreement:

The type of service and the purpose of processing are conclusively regulated in the product GT&C and the service specifications.

4 Evidence to be provided by Telekom

Telekom shall be free to prove the data protection obligations have been implemented in accordance with cipher 3.2 by providing the following evidence:

☒ compliance with the conventions permitted under Art. 40 GDPR;
☒ certification under a certification procedure in accordance with Art. 42 GDPR
☒ Current certificates, reports or excerpts from reports from independent instances (e.g., auditors, audit department);
☒ a suitable certification (except certificate according to Art. 42 GDPR)
☒ Affidavit by the processor.

Annex III Supplementary Terms and Conditions for Data Processing (STC-DP) for Open Telekom Cloud

Technical and organizational measures to provide the security of processing

1 Availability and resilience (Article 32 (1) letter b GDPR)

The "Availability" data protection goal refers to the requirement that personal data be accessible and can be processed, and that they can therefore 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.

a. Physical protection from external influences

Appropriate measures to protect against internal and external threats are formulated and implemented at the processor. These are designed to provide protection:

- against natural disasters, attacks, or accidents,
- against disruptions such as power failures or other supply issues,
- of cabling against interruption, malfunction, or damage.

Tests to ensure the effectiveness of the physical protection measures are carried out on a regular basis. The protection concept is also adapted in the event of changes to the processing of data. Relevant processes have been implemented at the processor.

b. Protection of the IT systems and networks from external threats

The processor has defined regulations that protect the IT systems, networks, and components (technical equipment, utilities, etc.) that are used for processing personal data against 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 make it possible for commissioned data processing to be contractually compliant even in adverse situations. The processor regularly reviews their effectiveness.

c. System hardening

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

- The patch level is up-to-date.
- When a system is installed, only those software components are installed or activated that are required for the system's operation and proper functioning.
- Apart from software functions, any hardware functions that are not required for the system's operation also remain deactivated after the system installation. 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 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, it has been safeguarded to prevent it (or the entire client/tenant with all of its services and data) from being deleted accidentally or by unauthorized persons.

d. Backup concept

The processor has defined regulations that enable a suitable backup strategy to be delivered. 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. Instead of a "classic" backup solution, it is

also possible to operate mirroring systems in a different security area, or even a combination of both strategies.

e. Personnel concept for ensuring the data protection goals

The processor has implemented a personnel concept that supports data protection by means of the following measures:

- Only specialist staff are used who have undergone the necessary training and accepted the obligations to maintain confidentiality and observe telecommunications secrecy.
- A responsible contact is defined for processing personal data. A deputization arrangement is in place.
- When their employment relationship, contract, or agreement ends, employees and processors return to the organization (controller/processor) any assets that are in their possession and were given to them to perform their task. These include means of access, computers, storage media, and mobile devices.
- Secrecy protection according to Section 203 StGB (Criminal Code) and social secrecy according to Section 35 SGB I (Social Code Book I) in a largely standardized manner.

f. 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 satisfies the following requirements/criteria:

- Rules are in place that define the time needed to restore regulated data processing following an incident.
- Resources for restoring data processing have been provided.
- Responsibilities have been assigned.
- Tested measures have been defined to protect against the incident and restore regular operation.
- Chains of information and escalation are in place.
- The way in which to interact with corresponding processes and regulations (backup concept, personnel concept, etc.) has been defined.

2 Integrity (Article 32 (1) letter b GDPR)

The "Integrity" data protection goal refers to the requirement that the data to be processed remain intact, complete, correct, and up-to-date.

a. Definition, use, and monitoring of the target behavior of processes

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

b. Authorization concept

The processor uses authorization concepts that specify who can access which systems, databases, or networks, and when. The authorization concepts should satisfy the following criteria:

- 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 access only to the networks, systems, and data for which they are explicitly authorized.
- A formal process for registering and deregistering has been defined so that access rights can be assigned.
- A formal process for granting user accesses has been defined 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.

c. 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. The objective of this measure is to ensure that such user accounts cannot be misused.

d. Crypto concept

The processor has defined the use of cryptographic measures to protect personal data through provisions. These provisions include:

- the use of the applied state of the art in cryptographic methods,

- the required protection level for personal data based on a risk assessment,
- the management and application of cryptographic keys,
- the protection of cryptographic keys throughout their lifecycle (generation, storage, application, and destruction).

The objectives of such a crypto concept are as follows:

- to ensure the integrity of sensitive data,
- to secure identity management processes,
- to support authorization processes,
- to ensure the confidentiality of sensitive data.

e. Processes for maintaining up-to-date data

The processor has defined, implemented, and communicated processes that support keeping personal data up-to-date and satisfy the following requirements:

- Requests for authorizations, changes, and deletions by the data subject are handled promptly and across all data records that are saved.
- Personal data are changed or deleted, either automatically or controlled by processes, across all data records that are saved.
- Any changes that are made to data with a personal reference can be differentiated from each other by means of a time stamp.
- Storage periods and deletion periods have been defined in accordance with statutory or contractual specifications.

3 Confidentiality (Article 32 (1) letter b GDPR)

The "Confidentiality" data protection goal refers to the requirement that no unauthorized person can access or use personal data.

a. Definition of the use of permitted resources and communications channels

The processor implements the following measures in such a way that the resources and communications channels that are used for processing personal data are defined:

- Areas are defined depending on the protection level and necessary 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 has been created and implemented at the organization on the basis of 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.
- Procedures that regulate the handling of data carriers are implemented in accordance with the protection level identified.
- If personal data are stored on mobile data carriers, they are effectively encrypted.
- 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 are 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).
- Suitable guidelines and measures to ensure confidentiality and integrity are implemented at the organization commensurate with the risks identified concerning the use of mobile devices (laptops, external storage media, cell phones). The aim of these rules is to minimize access to personal data, encrypt their storage and transmission, and reduce the use of external storage media to the absolute minimum.

b. Authentication method

Systems and applications are accessed by means of a suitable 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) are used. A high protection level is to be assumed if access to data is enabled that falls, for example, within Art. 9 (1) GDPR. If the protection level is low, username- and password-based authentication is implemented. 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, for example: passwords, PINs, (knowledge factor)/cryptographic keys, tokens, smartcards, OTP (possession factor)/or biometric features such as fingerprints or hand geometry (inherence).

- The specifications for creating passwords (length, complexity, reuse, etc.) are based, at the minimum, on the applied state of the art.
- 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 cryptographic one-way function (called "password hashing") that is appropriate for this purpose and has been classified as secure based on the applied state of the art.
- Where systems are used for managing and allocating passwords, these systems 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.

c. Obligation of employees

In connection with the processing of personal data agreed here, Telekom shall maintain confidentiality in accordance with the DSGVO, in accordance with § 3 TTDSG and in accordance with § 203 of the German Criminal Code (StGB) and shall obligate and sensitize the persons authorized to process the personal data accordingly. In the area of application of the processing of social data, Telekom will additionally commit to maintaining social secrecy in accordance with § 35 SGB I. Agreements in the GTC and the applicable documents to maintain confidentiality and protect non-personal data shall remain unaffected. Insofar as no agreement has been made in this respect in the General Terms and Conditions and the applicable documents, both parties undertake to keep secret all information from the area of the other party which is not generally public knowledge and which becomes known to them through the business relationship and not to use it for their own purposes outside this contract or the purposes of third parties.

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.

a. Definition and determination of the processing purpose

The processor uses appropriate measures to process the personal data processed on behalf of the controller 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
- and regulated change-of-purpose procedures.

b. Measures to ensure purpose limitation

The processor processes personal data exclusively for the contractually agreed purpose and gives access to the data only to persons/instances authorized to process 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, testing, and operating environments must be separated logically at the 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. Necessary exceptions to this rule are only possible if based on separate, written instructions from the customer.

c. Definition, implementation, and use of anonymization procedures

The processor organizes the data processing in such a way that personal data are processed only taking purpose limitation into account. If there is no purpose limitation, data that are not required are deleted. If it is not possible to delete the data, the relevant records are anonymized. Special-purpose pseudonyms, anonymization services, anonymous credentials, and the processing of pseudonymous or anonymized data are used for this; data masks are also implemented that suppress data fields, and there are also automatic lock and deletion routines, pseudonymization, and anonymization procedures.

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 are collected and processed when and for what purpose during a processing activity, which systems and processes are used for this, where the data flow for which purpose, and who has legal responsibility for the data and systems in the different data processing phases.

a. Record of procedures

The following requirement arising from Art. 30 GDPR was implemented at the processor's organization:
The "processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) [GDPR], the documentation of suitable safeguards;
- where possible, a general description of the technical and organizational security measures referred to in Article 32 (1) [GDPR].

The records referred to above shall be in writing, including in electronic form.
The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

The obligations referred to above shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10 [GDPR]."

b. 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.

c. Documentation and storage of contracts, agreements, and instructions

The processor stores all contracts, agreements, or instructions in such a way that they can be made available to the contracting parties or supervisory authorities within a reasonable period of time.

d. Logging of the data processing

Access by users and/or 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.

e. Ensuring obligations to furnish information

The processor has implemented a process that supports a data subject's right to information in accordance with the provisions of Art. 15 GDPR. This process is regularly checked to ensure its effectiveness.

6 Intervenability

The "Intervenability" data protection goal refers to the requirement that the data subject be 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.

a. Process implementation for implementing data subject rights

The processor has implemented measures for protecting data subject rights. In general, the measures specified below are appropriate:

- Unless already implemented by the controller, the processor has implemented a process for identifying and authenticating the persons who wish to exercise their data subject rights.
- The controller and processor jointly define a feature with which the data subject can be uniquely identified across organizational boundaries.
- The processor has implemented systems, software, and processes in such a way that measures can be taken to provide differentiated consent, withdrawal, and objection options.
- The processor has implemented an operational possibility for compiling, consistently rectifying, blocking, and deleting all information that was saved for a person.
- Preferential treatment is given to automated processing processes (not decision-making processes) that make access to the data that are processed expendable, and restrict the exertion of influence compared with processes that are dialog-controlled.

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

The processor observes the data subject rights and data protection requirements at the system design stage. The following measures are taken into consideration 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 retrieved by data subjects.
- Reduction in the processing options in processing steps.
- Creation of the required data fields, e.g., for lock indicators, notifications, consents, objections, 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.

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.

a. 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 been implemented:

- The attributes recorded in relation to the data subjects 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.

b. 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 appropriate:

- Restriction of the processing options in processing steps.
- Implementation of data masks that suppress data fields, and automatic lock and deletion routines, application of pseudonymization and anonymization procedures.
- Restriction of the options of accessing available data (display options, search fields, etc.) to the necessary minimum.

c. Definition, implementation, and control of a deletion concept

When processing personal data, the processor produces a deletion concept that includes the following:

- Specification of the data fields to be deleted
- Definition of deletion periods
- Control and proof of the deletion
- Responsible persons

8 Process for regularly testing, assessing, and evaluating (Article 32 (1) letter d GDPR; Article 25 (1) GDPR)

- Data protection management
- Incident response management
- Default settings that promote data protection (Article 25 (2) GDPR)
- Commission control

No commissioned data processing within the meaning of Article 28 GDPR without corresponding instructions from the customer, e.g., unequivocal drafting of the agreement, formalized commission management, stringent selection of the service provider, obligation to conduct thorough checks in advance, and follow-up check

Annex IV Supplementary Terms and Conditions for Data Processing (STC-DP) for Open Telekom Cloud

List of sub-processors (including sub-sub-processors)

The customer has authorized the use of the following sub-processors and sub-sub-processors in accordance with cipher 2 clause 7.7 letter a:

1 Approved sub-processors

Details about subprocessors/services/processing locations

Special approval:
Telekom intends to deploy the following subprocessors for the following services/at the following processing locations:

Deutsche Telekom TSI Hungary Kft.
1097 Budapest, Könyves Kalman 36
Services: Operation, 2nd level support
Processing location: Hungary

Deutsche Telekom ITTC Hungary Kft.
1097 Budapest, Könyves Kalman 36
Services: 2nd level support
Processing location: Hungary

Deutsche Telekom IT GmbH
53227 Bonn Landgrabenweg 151
Service: MyWorkplace
Processing location: Germany

Deutsche Telekom Systems Solutions Slovakia s.r.o.
040 01 Košice, Žriedlová 13
Service: Cloud provider
Processing location: Slovakia

T-Systems Multimedia Solutions GmbH
01129 Dresden, Riesaer Strasse 5
Service: IT-service provider
Processing location: Germany

T-Systems on site services GmbH
13509 Berlin, Holzhauser Str. 4-8
Service: IT-service provider
Processing location: Germany

operational services GmbH & Co. KG
60549 Frankfurt am Main,
Frankfurt Airport Center
Building 234 HBK25
Service: IT-service provider
Processing location: Germany

Deutsche Telekom Individual Solutions & Products GmbH
53113 Bonn, Friedrich-Ebert-Allee 70
Services: 1st level & 1.5 level support, hardware maintenance and setup
Processing location: Germany, Netherlands

GULP Solutions Services GmbH & Co. KG
50667 Cologne, Breite Strasse 137-139
Service: Service desk
Processing location: Germany
Deployed by Deutsche Telekom Individual Solutions & Products GmbH

I.T.E.N.O.S. International Telecom Network Operation Services GmbH
53119 Bonn, Lievelingsweg 125
Service: Hardware maintenance and setup
Processing location: Germany
Deployed by Deutsche Telekom Individual Solutions & Products GmbH

Deutsche Telekom Security GmbH
53113 Bonn, Bonner Talweg 100
Service: IT-Service provider
Processing location: Germany

ImpressSol GmbH
84072 Au i.d.Hallertau, Am Bahndamm 10
Service: Consulting
Processing location: Germany