Supplementary Terms and Conditions for Commissioned Processing (ErgB-AV) for Open Telekom Cloud

The agreement is concluded between T-Systems International GmbH (hereinafter referred to as Telekom), Hahnstraße 43d, 60528 Frankfurt am Main, Germany and the customer.

1 General information

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 GT&C and other applicable Telekom documents) is carried out by Telekom for the customer within the meaning of the applicable data protection laws. For clarification, although the customer is referred to as the controller in this agreement, the customer may act either as a controller or as a processor for data processed by the customer on behalf of its own customers. In this case, Telekom acts as a subprocessor of the customer.

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

The specific contractual parties, 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 GT&C, the other applicable documents, these "Supplementary Terms and Conditions for Commissioned Processing" and their appendices ("ErgB-AV").

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 item 2 with the respective selected option in the original text. The standard contractual clauses of the EU Commission may not be modified in the text of sections I and II according to the mandatory requirements of the EU Commission and must be reproduced unchanged in their original text. Deviations are explicitly outlined in section III, item 3. Item 7.8 has been amended by section III, clause 3.4 to ensure that data processing does not take place in third countries without an adequacy decision (Article 45 GDPR). The regulation of audit rights in item 7.6.b has been further modified by section III, item 3.2, and item 7.7.a "Subcontractors" has been further amended by section III, item 3.3.

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

2 Standard contractual clauses of the EU ("clauses")

SECTION I

Clause 1 [Purpose and scope]

a) These standard contractual clauses of the EU ("clauses") are intended to ensure compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (the General Data Protection Regulation) [OPTION 1].

b) Controllers and processors listed in Appendix I have agreed to these clauses to ensure compliance with Article 28 (3) and (4) of Regulation (EU) 2016/679, and/or Article 29 (3) and (4) of Regulation (EU) 2018/1725.

c) These clauses apply to the processing of personal data as specified in Appendix II.

d) Appendices I to IV are an integral part of the clauses.

e) These clauses are applicable regardless of the obligations to which the controller is subject under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These clauses do not in themselves ensure compliance with the obligations relating to international data transfers under Chapter V of Regulation (EU) 2016/679.

Clause 2 [Unchangeability of clauses]

a) The parties undertake not to amend the clauses except to supplement or update the information specified in the appendices.

This shall not prevent the parties from incorporating the standard contractual clauses of the EU set forth in these clauses into a more comprehensive contract and from adding further clauses or additional guarantees, provided that it does not directly or indirectly conflict with the clauses or interfere with the fundamental rights or freedoms of the data subjects.

Clause 3 [Interpretation]

a) Where terms defined in Regulation (EU) 2016/679 are used in those clauses, those terms shall have the same meaning as in the relevant Regulation.

b) These clauses shall be interpreted in accordance with the provisions of Regulation (EU) 2016/679.

c) These clauses shall not be interpreted in a manner contrary to the rights and obligations provided for in

Regulation (EU) 2016/679 or in such a way as to restrict the fundamental rights or freedoms of data subjects.

Clause 4 [Precedence]

In the event of any conflict between these clauses and the provisions of any related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

Clause 5 [Tying clause]

n/a

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 for which the personal data are processed on behalf of the controller, are set out in Appendix II.

Clause 7 [Obligations of the parties]

7.1 Instructions

a) The processor shall only process personal data on the documented instructions of the controller, unless it is obligated to process under European Union law or the law of a member state to which it is subject. In such a case, the processor shall notify the controller of such legal requirements prior to the processing, insofar as the relevant law does not prohibit this due to significant public interest. The controller may issue further instructions throughout the processing of personal data. These instructions must always be documented.

b) The processor shall inform the controller without undue delay if it considers that instructions given by the controller infringe Regulation (EU) 2016/679 or 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) laid out in Appendix II, unless it receives further instructions from the controller.

7.3 Duration of processing personal data

The data shall be processed by the processor only for the duration specified in Appendix II.

7.4 Security of processing

a) The processor shall take at least the technical and organizational measures listed in Appendix III to ensure the security of the personal data. This includes the protection of data against a breach of security that results, whether accidentally or unlawfully, in the destruction, loss, alteration, or unauthorized disclosure of or access to the data (hereinafter referred to as "personal data breach"). In assessing the appropriate level of protection, the parties shall take due account of the state of the art, the costs of implementation, the nature, scope, circumstances, and purposes of the processing, as well as the risks involved for the data subjects.

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

7.5 Sensitive data

If the processing concerns personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or containing genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning a person's health, sexual conduct, or sexual orientation, or data concerning criminal convictions and offenses (hereinafter referred to as "sensitive data"), the processor shall apply specific restrictions and/or additional safeguards. The same applies to social data in accordance with § 67 (2) SGB X, § 35 (4) SGB I.

7.6 Documentation and compliance with clauses

a) The parties must be able to demonstrate compliance with these clauses.

b) The processor shall promptly and appropriately handle requests from the controller regarding the processing in accordance with these clauses.

c) The processor shall provide the controller with all information necessary to demonstrate compliance with the obligations set out in these clauses and arising directly from Regulation (EU) 2016/679. At the request of the controller, the processor shall also permit and contribute to the audit of the processing activities covered by these clauses at reasonable intervals or when there are indications of non-compliance. When deciding on a review or audit, the controller may consider relevant certifications of the processor.

d) The controller may conduct the audit themselves or may engage an independent auditor. Audits may include inspections of the processor's premises or physical facilities and shall be conducted with reasonable advance notice, as appropriate.

e) The parties shall make available to the relevant supervisory authority or authorities, upon request, the information referred to in this clause, including the results of audits.

7.7 Use of subcontracted processors

a) GENERAL WRITTEN AUTHORIZATION: The processor shall have the general authorization of the controller to engage subprocessors that are included in an agreed list. The processor shall expressly inform the controller in writing at least four weeks in advance of any intended changes to this list by adding or replacing subprocessors, thereby giving the controller sufficient time to object to such changes before engaging the relevant subprocessor(s). The processor shall provide the controller with the necessary information to

enable the controller to exercise its right to object. [OPTION 2]

b) If the processor entrusts a subprocessor with the performance of certain processing activities (on behalf of the controller), such subcontracting must be made by way of a contract that imposes on the subprocessor substantially the same data protection obligations as those applicable to the processor under these clauses. The processor shall ensure that the subprocessor complies with the obligations to which the processor is subject in accordance with these clauses and in accordance with Regulation (EU) 2016/679.

c) The processor shall provide the controller with a copy of any such subcontracting agreement and any subsequent amendments upon the controller's request. To the extent necessary to protect trade secrets or other confidential information, including personal data, the processor may obscure the wording of the agreement prior to providing a copy.

d) The processor shall be fully liable to the controller for the subprocessor's compliance with its obligations under the contract concluded with the processor. The processor shall notify the controller if the subprocessor fails to fulfill its contractual obligations.

e) The processor shall agree with the subprocessor on a third party beneficiary clause, according to which the controller – in case the processor ceases to exist factually or legally or is insolvent – has the right to terminate the subcontract and instruct the subprocessor to delete or return the personal data.

7.8 International data transfers to third countries without an adequacy decision (no transfer to third countries takes place, therefore the scope of the following clause is <u>not</u> applicable, see clauses section III 3.4. and section IV Approved subprocessors).

a) Any transfer of data by the processor to a third country or an international organization shall be made solely on the basis of documented instructions from the controller or to comply with a specific provision under European Union law or the law of a member state to which the processor is subject and shall comply with Chapter V of Regulation (EU) 2016/679.

b) The controller agrees that in cases where the processor uses a subprocessor pursuant to clause 7.7 for the performance of certain processing activities (on behalf of the controller) and such processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the subprocessor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46 (2) of Regulation (EU) 2016/679, provided that the conditions for the application of such standard contractual clauses are met.

Clause 8 [Support of the controller]

a) The processor shall inform the controller without undue delay of any request received from the data subject. It shall not answer the request itself, unless it has been authorized to do so by the controller.

b) Taking into account the nature of the processing, the processor shall assist the controller in fulfilling the controller's obligation to respond to requests from data subjects to exercise their rights. In fulfilling its obligations under letters a and b, the processor shall follow the instructions of the controller.

c) In addition to the processor's obligation to assist the controller under clause 8 letter b, the processor shall, taking into account the nature of the data processing and the information available to it, also assist the controller in complying with the following obligations:

1) Obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (hereinafter referred to as "data protection impact assessment") where a form of processing is likely to result in a high risk to the rights and freedoms of natural persons;

2) Obligation to consult the competent supervisory authority (or authorities) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk, unless the controller takes measures to mitigate the risk;

3) Obligation to ensure that personal data is factually accurate and up to date, by the processor notifying the controller without undue delay if it discovers that the personal data it processes is inaccurate or out of date;

4) Obligations under Article 32 of Regulation (EU) 2016/679. [OPTION 1]

d) The parties shall specify in Appendix III the appropriate technical and organizational measures for the processor's assistance to the controller in the application of this clause and the scope and extent of the assistance required.

Clause 9 [Personal data breach notification]

In the event of a personal data breach by the controller, the processor shall cooperate with and provide appropriate assistance to the controller to enable the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, taking into account the nature of the processing and the information available to the processor.

9.1 Breach of the protection of the data processed by the controller

In the event of a personal data breach in connection with the data processed by the controller, the processor shall assist the controller in the following ways:

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

b) By obtaining the following information to be included in the notification of the controller in accordance with Article 33 (3) of Regulation (EU) 2016/679 [OPTION 1]; this information shall include at least the following:

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

2) The probable consequences of the personal data breach;

3) The measures taken or proposed by the controller to address the personal data breach and, where appropriate, measures to mitigate its possible adverse effects. If and to the extent that all such information cannot be provided at the same time, the initial notification shall include the information available at that time, and additional information, when it becomes available, shall be provided thereafter without unreasonable delay;

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

9.2. Breach of the protection of the data processed by the processor

In the event of a personal data breach in connection with the data processed by the processor, the processor shall notify the controller thereof without undue delay after becoming aware of the breach. This notification must contain at least the following information:

a) A description of the nature of the breach (specifying, if possible, the categories and approximate number of data subjects affected, and the approximate number of records concerned);

b) Contact details of a point of contact where further information on the personal data breach can be obtained;

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

If and to the extent that all such information cannot be provided at the same time, the initial notification shall include the information available at that time, and additional information, when it becomes available, shall be provided thereafter without unreasonable delay.

The parties shall specify in Appendix III any other information to be provided by the processor to assist the controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 [OPTION 1].

SECTION III

FINAL PROVISIONS

Clause 10 [Violations of the clauses and contract termination]

a) If the processor fails to comply with its obligations under these clauses, the controller may, irrespective of the provisions of Regulation (EU) 2016/679, instruct the processor to suspend the processing of personal data until it complies with these clauses or the contract is terminated. The processor shall inform the controller without undue delay if, for whatever reason, it is unable to comply with these clauses.

b) The controller shall be entitled to terminate the contract insofar as it concerns the processing of personal data according to these clauses if

1) The controller has suspended the processing of personal data by the processor in accordance with letter a and compliance with these clauses has not been restored within a reasonable period of time and in any case within one month after the suspension;

2) The processor materially or persistently violates these clauses or fails to comply with its obligations under Regulation (EU) 2016/679;

3) The processor fails to comply with a binding decision issued by a competent court or the competent supervisory authority (authorities) which has as its subject matter its obligations under these clauses, Regulation (EU) 2016/679.

c) The processor shall be entitled to terminate the contract insofar as it concerns the processing of personal data pursuant to these clauses if the controller insists on the performance of its instructions after having been notified by the processor that its instructions violate applicable legal requirements in accordance with clause 7.1 letter b.

d) Upon termination of the contract, the processor shall, at the discretion of the controller, erase all personal data processed on behalf of the controller and certify to the controller that this has been done, or return all personal data to the controller and erase existing copies, unless there is an obligation under European Union or member state law to retain the personal data. Until the data is erased 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 GTC, other applicable documents, and these ErgB-AV. 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 from the controller can be given within the agreed scope of the standard product and must be documented by the customer. In the event of further instructions from the controller that go beyond the agreed scope, item 4 of this ErgB-AV (Amendments) shall apply.

3.2 [Supplement to clause 7.6.]

The customer is permitted to conduct routine on-site inspections of the processor twice per calendar year. The right to conduct on-site inspections for specific reasons (e.g., data protection breaches, violations of legal and/or contractual data protection provisions) remains unaffected. The customer shall primarily assess whether the performance of non-event-driven on-site inspections can be replaced by the submission of documents, evidence, certifications, or audits to demonstrate compliance with the clauses as well as the obligations set forth in these clauses and directly arising from Regulation (EU) 2016/679. Non-event-driven on-site inspections must be announced in advance in a timely manner. Disruptions to business operations must be avoided.

Persons or third parties entrusted with the inspection by the customer shall be obliged to maintain confidentiality in a documented form upon assignment. Third parties within the meaning of this paragraph may not be representatives of competitors of Telekom.

3.3 [Approved subprocessors]

The list of subprocessors approved by the controller (GENERAL WRITTEN AUTHORIZATION in accordance with clause 7.7 letter a) can be found in Appendix IV. The processor shall inform the controller six weeks in advance in writing of any planned changes to subprocessors that process the customer's data on behalf of the processor and shall provide the controller with the information it requires to exercise its right to object. The controller shall inform the processor in writing within four weeks whether they object to the proposed change. If the controller does not object to the change within four weeks of being notified, the change shall be deemed approved. The controller shall not unreasonably object to such a change. If the controller objects and this makes it impossible for the processor to provide its services, the controller may terminate the affected services without notice within one month of the notification of the change (special termination right). In the event of the legitimate exercise of the special termination right due to the non-approval of a subcontractor change for good cause, the processor may not involve the new subcontractor in processing the client's data until the completion of the transition phase (migration to an alternative, legally compliant infrastructure) by the controller. This transition phase must not exceed six months for both parties, during which the processor's internal alternatives shall be prioritized and evaluated. Both parties commit to making their best efforts to find a mutually agreeable solution.

During the transition phase, the processor reserves the right to isolate the client's environment in such a way that access by any of the subprocessors affected by the objection is technically impossible. The processor is responsible for providing the client with the corresponding proof. Once this proof has been provided, the client has no right to demand that the processor not deploy the subprocessor affected by the objection outside of the isolated environment. The

processor is not obligated to maintain the isolated environment beyond the migration phase.

3.4 [International data transfer]

A data transfer to insecure third countries without an adequacy decision or access from insecure third countries does not take place. Clause 7.8 is replaced with:
The processor shall not transfer data to a third country without an adequacy decision by the EU Commission pursuant to Article 45 GDPR.

3.5 [Assignment of terms]

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 sense.

3.6 [Supplement to clause 10 d) and Article 28 (3) g) GDPR]

The parties agree that clause 10 letter d and Article 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 ErgB-AV 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 ErgB-AV, the place of jurisdiction is that which has been agreed in the GT&C. If the GT&C 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 ErgB-AV agreement and the provisions of other agreements, in particular the GT&C and the other applicable documents, the provisions of this ErgB-AV agreement shall prevail. In all other respects the provisions of the GT&C and the other applicable documents shall remain unaffected and shall apply to this ErgB-AV accordingly.

Appendix I Supplementary Terms and Conditions for Commissioned Processing (ErgB-AV) for Open Telekom Cloud (OTC)

List of parties

The parties to the agreement are the contractual partners of the service agreement.

Appendix II Supplementary Terms and Conditions for Commissioned Processing (ErgB-AV) for Open Telekom Cloud (OTC)

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 (Article 9 GDPR, Article 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 process or collect the personal data by transmitting this data to Telekom via a secure internet-based IP-VPN 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, such as maintenance or troubleshooting, and it only occurs with the customer's explicit approval.

3 Processing purpose

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 item 3.2 by providing the following evidence:

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

Appendix III Supplementary Terms and Conditions for Commissioned Processing (ErgB-AV) for Open Telekom Cloud

Technical and organizational measures to ensure the security of processing

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

a. Physical protection from external influences

Appropriate measures to protect against internal and external threats are formulated and implemented at the processor's end. 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 in accordance with the specifications of the manufacturer/supplier.
- 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, and 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 for its area of responsibility 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 shall be 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.

- Obligation of staff to maintain confidentiality in accordance with § 203 of the German Criminal Code (StGB) and social secrecy in accordance with § 35 of Book 1 of the German Social Code (SGB 1).

f. Creation of an emergency concept to restore a processing activity

The processor has implemented an emergency concept to restore data processing in its area of responsibility. 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)

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 requirements, 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 in its area of responsibility to protect personal data through provisions. This 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,
- and 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 forcorrections, changes, and deletions 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)

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 that specify and implement the necessary security perimeters.
- 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 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.
- If personal data are stored on mobile data carriers, they are effectively encrypted.
- 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. 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 administrator access, 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. Employee obligations

In connection with the processing of personal data agreed herein, Telekom shall maintain confidentiality in accordance with the GDPR, § 3 of the German Telecommunications Digital Services Data Protection Act (TDDDG) and § 203 StGB, and shall oblige and raise the awareness of the persons authorized to process the personal data accordingly. Within the scope of processing social data, Telekom shall additionally commit to maintaining social secrecy in accordance with § 35 SGB I. Any agreements in the GT&C and the other applicable documents regarding the maintenance of confidentiality and the protection of non-personal data shall remain unaffected. Insofar as no agreement in this regard has been made in the GT&C and the other applicable documents, both parties shall treat as confidential all information relating to the other party that is disclosed to them during the course of the business relationship, and is not common knowledge, and shall not use this information for purposes of their own that fall outside the scope of this agreement or for the purposes of any third party.

4 No data chaining

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.
- In case that 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.

5 Transparency

a. Record of procedures

Article 30 GDPR has been implemented at the processor's end.

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

- **Process implementation for implementing data subject rights**

The processor has implemented measures for protecting data subject rights during processing. Systems, software, and processes have been implemented in such a way that differentiated consent, withdrawal, and objection options are available.

.

7 Data minimization

The processor only processes personal data that is strictly necessary for the purpose of the processing.

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;
-
- Job control
- No commissioned data processing within the meaning of Article 28 EU 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, follow-up checks.

Appendix IV Supplementary Terms and Conditions for Commissioned Processing (ErgB-AV) for Open Telekom Cloud

List of subprocessors (including sub-subprocessors)

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

1 Approved subprocessors

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

Deutsche Telekom MMS 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: Development services
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 71-77
Services: 1st level & level 1.5 support, hardware maintenance and setup
Processing location: Germany, Netherlands

Deutsche Telekom Security GmbH
53113 Bonn, Friedrich-Ebert-Allee 71-77
Service: IT service provider
Processing location: Germany

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

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

Deutsche Telekom Systems Solutions Slovakia s.r.o.
040 11 Košice, Moldavská cesta 8B
Service: Cloud provider
Processing location: Slovakia

SC Combridge S.R.L
520023 Sfantu Gheorghe, Jud. Covasna
Str. Gödri Ferenc Nr. 18
Service: Cloud provider
Processing location: Romania

T-Systems ITC Iberia, S.A.
08020 Barcelona, Pere IV 313
Services: Operation, 2nd Level Support
Processing location: Spain