Supplementary Terms and Conditions for Commissioned Processing (Sup-CP) for Microsoft Online Services (Office 365/Dynamics 365/Azure)

These CP terms refer to the services of Telekom, in particular to product provision, billing, and support. Data storage by Microsoft is not included in the scope of this CP.

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 GTC and other applicable Telekom documents) is carried out by Telekom for the customer within the meaning of the applicable data protection laws.

This agreement is intended to ensure 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 GTC, the other applicable documents, these "Supplementary Terms and Conditions for Commissioned Processing" and the related appendices ("Sup-CP").

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.

Further provisions within the meaning of clause 2 letter b are agreed by the parties in items 3, 4, and 5 of this Sup-CP. The regulations take particular account of the fact that Telekom's service is a standardized GTC 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) These standard contractual clauses ("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.

b) This shall not prevent the parties from incorporating the standard contractual clauses 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]

a) An entity that is not a party to these clauses may, with the consent of all parties, join these clauses as a controller or processor at any time by completing the appendices and signing Appendix I.

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

b) Upon completion and signature of the appendices referred to in letter a, the joining entity shall be treated as a party to these clauses and shall have the rights and obligations of a controller or processor as designated in Appendix I.

c) No rights or obligations arising from these clauses shall apply to the joining entity for the period prior to its accession as 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 for which the personal data are processed on behalf of the controller, are set out in Appendix II.

Clause 7 [Obligations of the parties]

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.

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 accidental or unlawful, 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.

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

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

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

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, 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

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

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 Sup-CP. 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, item 4 of this Sup-CP (Amendments) shall apply.

3.2 [Supplement to clause 7.6.]

With regard to clause 7.6, the parties agree that the controller shall use suitable certifications from Telekom and other documents submitted by Telekom 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

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

inspection in exceptional cases that require special justification.

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.

3.4 [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.

3.5 [Supplement to clause 7.8.]

With regard to clause 7.8, the parties state that insofar as the processor has concluded the standard data protection clauses with its subprocessors as of 2010 and, if necessary, has taken supplementary measures, and therefore the business is existing business within the meaning of the Commission's implementing decision of June 4, 2021, these existing standard data protection clauses shall continue to apply until further notice. The processor shall, to the extent possible, replace these standard data protection clauses as of 2010 with the standard data protection clauses as of 2021 no later than December 27, 2022. The parties agree that this approach represents a condition in conformity with the contract and the law.

3.6 [Implementation]

Insofar as the implementation of the standard data protection clauses as of 2021 with subcontracted processors in the third country cannot be carried out by December 27, 2022, the provisions of clause 7.7 on the use of subcontracted processors and item 4.1 on amendments shall apply for establishing a legally compliant situation by Telekom.

3.7 [Transfer to third countries]

In the event of a third country transfer, the processor is also entitled to use approved suitable safeguards with its subcontractors (Appendix IV) in accordance with Article 46 of the GDPR, in particular approved binding internal data protection rules in accordance with Article 47 of the GDPR.

3.8 [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 Changes

Any changes to this Sup-CP agreement and any side agreements shall be made in writing (including in electronic form). This shall also apply to the waiver of this written form clause itself.

The following regulations shall apply exclusively and conclusively for changes to the Sup-CP. They take precedence over other regulations, e.g., regulations established in the GTC for changes to services, prices, or legal conditions. Clause 7.7 letter a, sentence 2, shall apply to changes to subprocessors.

4.1 [Changes made by Telekom]

If Telekom intends to amend the agreed services or conditions for commissioned processing (e.g., due to decisions by authorities, changes in supplier relationships, legal amendments), it shall inform the customer in writing (e.g., by letter or email) a minimum of four weeks before the amendments take effect and prevent any disadvantages for the customer where possible. The amended conditions will become part of the agreement subject to the following requirements:

In the event of amendments which benefit the customer, in the event of minor importance, or in the event of binding legal changes, Telekom is entitled to make unilateral amendments to the processing conditions. For all other amendments, the customer has the right to terminate the services affected when the amendments take effect, without adhering to the notice period. The customer's right of termination shall be expressly referred to in the notification about the amendments.

4.2 [Changes by the customer]

If the customer wishes to amend the services or conditions for commissioned processing, they shall inform Telekom and give reasons for the desired change. Telekom shall send a proposal subject to charge to the customer for approval in the event that extensive amendments are desired.

If Telekom agrees to the customer's desired amendments in return for additional remuneration, if applicable, Telekom will send them the amended documents. The changes will come into effect at the time stated in the documents if the customer accepts them within four weeks. If Telekom rejects the customer's desired amendments or can only deliver them at a significantly higher cost, it shall inform the customer of this. In such a case, the customer is entitled to terminate the service affected without adhering to a notice period.

In the event of a termination, the customer shall be obligated to pay Telekom a compensation payment amounting to 50 percent of the monthly charges still due up to the end of the minimum contract term which had been agreed. The compensation payment shall not be payable or shall be lower if the customer can verify that the damage suffered by Telekom was significantly lower or that no damage was suffered at all. The compensation payment shall not be payable provided that the customer has been instructed to suspend the transfer of data by its supervisory authority.

4.3 [Continued validity of existing regulations]

The existing provisions shall continue to apply unchanged and Telekom is not obligated to implement any changes until an agreement has been reached regarding the customer's desired changes or the termination of the services affected.

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

4.4 [Suspension of data processing]

The customer is entitled to demand data processing be suspended until an agreement has been reached regarding its desired changes or the termination of the services affected. They shall still be obligated to pay the agreed remuneration.

5 Miscellaneous

5.1 [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.

5.2 [Validity of the agreement]

The invalidity of a provision of this Sup-CP 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.

5.3 [Place of jurisdiction]

For disputes in connection with this Sup-CP, the place of jurisdiction is that which has been agreed in the GTC. If the GTC 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.

5.4 [Priority regulation]

In the event of contradictions between the provisions of this Sup-CP agreement and the provisions of other agreements, in particular the GTC and the other applicable documents, the provisions of this Sup-CP agreement shall prevail. In all other respects the provisions of the GTC and the other applicable documents shall remain unaffected and shall apply to this Sup-CP accordingly.

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

Appendix I Supplementary Terms and Conditions for Commissioned Processing (Sup-CP) for [Microsoft Online Services (Office 365/Dynamics 365/Azure)]

List of parties

The parties to the agreement are the contractual partners of the Sup-CP.

Appendix II Supplementary Terms and Conditions for Commissioned Processing (Sup-CP) for [Microsoft Online Services (Office 365/Dynamics 365/Azure)]

Description of the processing

A commissioned processing agreement (CPA) with Microsoft according to Article 28 GDPR is concluded at the time of product activation or renewal of the product license and is part of the software terms of use of the manufacturer (Microsoft Customer Agreement MCA, Online Service Terms, and the actual Licensing Terms for the respective product).

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

☒ Interested parties of the controller

☒ Suppliers of the controller

☒ Employees of external companies

c. Category of personal data:

☒ Master data of the controller’s customers

☒ Contact data of the controller’s customers

☒ Master data of the controller’s employees

☒ Contact data of the controller’s employees

☒ All other personal data that the customer has processed within the scope of the service under contract

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 provides Telekom with the personal data, enables Telekom to access the personal data, or allows Telekom to process the personal data as described below:

☒ Transmission by the customer via secured connection: https:// and VPN connection to Microsoft Online Services.

☒ Access via a Secure Data Room:
When batch importing or batch exporting the customer’s customer data to and from Microsoft Online Services

☒ Encrypted transmission via:
Standard SQL Server-cell level encryption
or HTTPS TLS/SSL:
https://learn.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365?view=o365-worldwide

and/or:

☒ Maintenance, remote maintenance, or fault analysis services:

For set-up or service incidents: transfer via a secure connection, encrypted email for access to the Dynamics 365 platform and its online service applications, for data collection via a special interface (e.g., via the customer’s CRM import data or manual entry by the customer or customer support themselves).

This data shall be provided to Telekom as set out in § 5 (5.1) e) and h) “The customer’s duties to cooperate” and well as

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

§ 16 “Data protection” of the General Terms and Conditions for IT Services.

☒ Software testing/maintenance via remote access for the following software product(s):

Microsoft Dynamics 365 online services

☒ Testing and maintenance work on workstation systems shall be carried out upon approval by the relevant authorized person/affected employee of the customer.

☒ A separate notification (by email/telephone/in writing) about imminent test and maintenance work shall be sent to the customer by Telekom before the beginning of the work.

☒ At the customer's request, Telekom will provide information on what work will be carried out, when and by which Telekom employees. Telekom lets the customer know how these persons will identify and authenticate themselves to the customer.

☒ If necessary, the contractual parties shall reach a mutual understanding about data protection measures that may be necessary in the customer's/Telekom's respective areas of responsibility.

☒ Telekom shall make use of the access rights granted to it in such a way – including with regard to timing – that is necessary for the proper performance of the commissioned maintenance and testing tasks.

3 Processing purpose

The services are described in detail in the customer’s duties to cooperate in § 5 and in § 16 “Data protection” of the General Terms and Conditions for IT Services (applicable document).

4 Processing sites in third countries

If commissioned processing is carried out in a third country, this is listed in Appendix IV Supplementary Terms and Conditions for Commissioned Processing (Sup-CP).

5 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.

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.

Appendix III Supplementary Terms and Conditions for Commissioned Processing (Sup-CP) for [Microsoft Online Services (Office 365/Dynamics 365/Azure)]

Technical and organizational measures to ensure the security of processing

The following measures shall be agreed for the commissioned collection and/or processing of personal data:

a) Availability

- **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.

- **Protection of the IT systems and networks from external influences**

The processor has defined rules to protect IT systems, networks, and components from unauthorized access, unauthorized modification, loss, or destruction. 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.

- **Resilience of systems and services**

Information-processing systems and services are protected against malware, and resilience is increased through system hardening.

- **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.

- **Emergency concept to recover a processing activity**

The processor has implemented an emergency concept for recovery after a data processing disruption.

b) Integrity

- **Definition, use, and monitoring of the target behavior of processes**

The processor has defined processes for implementing data protection and information security. The objective of these specifications is to implement the processing of personal data in such a way that a defined target behavior of the processes is guaranteed. The provisions are reviewed regularly to ensure they are effective, up-to-date, and compliant with regulations.

- **Authorization concept**

The processor uses authorization concepts that specify bindingly who can access which systems, databases, or networks, and when.

- **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.

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.

- **Crypto concept**

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

  - the use of the applied state of the art in cryptographic methods,
  - the management and application of cryptographic keys,
  - the protection of cryptographic keys throughout their lifecycle (generation, storage, application, and destruction).

- **Processes for maintaining up-to-date data**

The processor has defined processes that support up-to-date data through the following measures:

  - Requests for authorizations, changes, and deletions by the data subject are handled promptly and across all data records that are saved.
  - Storage periods and deletion periods have been defined in accordance with statutory or contractual specifications and are implemented.

c) Confidentiality

- **Employee obligations**

The employees have been obligated to maintain data privacy and information protection.

- **Definition and monitoring of the use of permitted resources and communications channels**

The processor implements measures so that the resources and communication channels used for the processing of personal data are defined and their use is monitored:

  - Appropriate physical access control policies are defined and applied so that only authorized persons are granted access to areas where processing takes place.
  - A system access control policy has been created and implemented at the organization on the basis of data protection requirements. This policy regulates access to personal data depending on the required protection level and on a need-to-know basis.
  - Policies, security procedures, and control measures exist to adequately protect the transmission and transport of information.

- **Secure authentication procedures**

Access to systems and applications is protected by an appropriately secure authentication procedure that takes into account the protection level of the personal data. If the level of protection required is high (e.g., pursuant to Article 9 (1) GDPR), login procedures based on possession and knowledge (two-factor authentication) are used as a matter of priority.

d) No data chaining

- **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.

- **Measures for ensuring 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. The following measures have been taken to avoid chaining of records with different purposes:

  - Separation by organizational/departmental boundaries
  - Segregation of processing by tenant

e) Transparency

- **Record of procedures**

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

- **Documentation of the data processing**

The processing process is documented in such a way that it is clear how personal data is processed.

- **Logging of the data processing**

Access by users and system administrators to personal data must be logged and regularly checked, taking the principle of data minimization and the protection level into account.

- **Ensure obligations to furnish information**

The processor has implemented a process that supports a data subject's right to information in accordance with Article 15 GDPR.

f) 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.

g) Data minimization

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

- Pseudonymization and anonymization procedures are used.
- Options for taking note of existing data (display options, search fields, etc.) have been limited to the necessary minimum.

Appendix IV Supplementary Terms and Conditions for Commissioned Processing (Sup-CP) for [Microsoft Online Services (Office 365/Dynamics 365/Azure)]

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

Subprocessor:

Deutsche Telekom IT GmbH
Landgrabenweg 151, 53227 Bonn, Germany
Service: Platform operator of Telekom Cloud Marketplace
Processing location: Germany

T-Systems International GmbH
Hahnstr. 43d, 60528 Frankfurt am Main, Germany
Service: Hosting the Telekom Cloud Marketplace
Processing location: Germany

Deutsche Telekom Service GmbH
Friedrich-Ebert-Allee 71-77, 53113 Bonn, Germany
Services: 1st and 2nd level support
Processing location: Germany

Telekom intends to commission (further) subprocessors. The actual names are available on request or can be requested via GDPR@telekom.de.

2 Approved sub-subprocessors

None.

Please note that any sub-subprocessors of Microsoft are not part of these Supplementary Terms and Conditions for Commissioned Processing between Telekom and the customer.

This document is a convenience translation of the German original. In case of discrepancy between the English and German versions, the German version shall prevail.