Supplementary Terms and Conditions for Data Processing (STC-DP) 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 General Terms & Conditions and other applicable Telekom documents) is carried out by Telekom for the customer within the meaning of the applicable data protection laws.

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

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

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

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

2 Standard contractual clauses ("clauses")

SECTION I

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

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

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

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

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

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

Clause 2 [Invariability of the Clauses]
a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

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

Clause 3 [Interpretation]
a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

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

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

Clause 4 [Hierarchy]
In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 [Docking clause]
a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

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

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

SECTION II

Obligations of the parties

Clause 6 [Description of processing]
The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7 [Obligations of the parties]
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 Annex II.

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

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

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

7.3 Duration of the processing of personal data
Processing by the processor shall only take place for the duration specified in Annex II.

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

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

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

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

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

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

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

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

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

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

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

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

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

7.8 International transfers

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

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

Clause 8 [Assistance to the controller]

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

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

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

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

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

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

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

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

Clause 9 [Notification of personal data breach]

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

9.1 Data breach concerning data processed by the controller

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

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

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

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

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

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

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

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

9.2 Data breach concerning data processed by the processor

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

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

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

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

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

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

SECTION III

FINAL PROVISIONS

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

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

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

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

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

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

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

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

3 Other clauses within the meaning of clause 2 b

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

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

3.3 [Approved sub-processors]
The list of sub-processors approved by the controller (GENERAL WRITTEN AUTHORIZATION in accordance with clause 7.7 letter a) can be found in Annex IV.

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

3.5 [Realization]
To the extent that the standard data protection clauses with subcontracted processors in the third country cannot be implemented, the provisions of clause 7.7 on the use of subcontracted processors and cipher 4.1 on amendments shall apply for establishing a legally compliant situation by Telekom.

3.6 [Third country transfer]
In the event of a third country transfer, the processor is also entitled to use approved suitable safeguards with its subcontractors (Annex IV) in accordance with Art. 46 of the GDPR, in particular approved binding corporate protection rules in accordance with Art. 47 of the GDPR.

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

4 Changes

Any changes to this STC-DP 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 STC-DP. They take precedence over other regulations, e.g., regulations established in the General Terms & Conditions for changes to services, prices, or legal conditions. Clause 7.7 letter a, sentence 2, shall apply to changes to sub-processors.

4.1 [Changes made by Telekom]
If Telekom intends to change the agreed services or conditions of the commissioned data processing (e.g., due to decisions by authorities, changes in supplier relationships, legal amendments), they shall inform the customer in writing (e.g., by letter or email) a minimum of 4 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 changes 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 conditions of the commissioned data processing. 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 adjust the services or conditions of the commissioned data 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 adjusted documents. The changes will come into effect at the time stated in the documents if the customer accepts them within 4 weeks. If Telekom rejects the customer's desired adjustments or can only deliver them at a significantly higher cost, they 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 % 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 damages suffered by Telekom were significantly lower or that no damages were 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.

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

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

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

Annex I Supplementary Terms and Conditions for Data Processing (STC-DP) for Microsoft Online Services (Office 365/Dynamics 365/Azure)

List of parties

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

Annex II Supplementary Terms and Conditions for Data Processing (STC-DP) 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 (Art. 9 GDPR, Art.10 GDPR) that take full account of the sensitivity of the data and the associated risks (e.g. additional security measures):

None.

2 Access to personal data

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

☒ Transfer by the customer via a secure 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 transfer 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 services, remote maintenance or fault analysis:
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 § 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

The following additional agreements have been reached:

☒ 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 respective areas of responsibility of Telekom/the customer.

☒ 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 Duration of processing

☒ Necessity for service provision

☒ Statutory retention periods

☒ Statutory deletion periods

4 Processing purpose

The services are described in detail in the customer’s duties to cooperate in § 5 and in § 15 “Data protection” of the General Terms and Conditions for IT Services (applicable document).

5 Processing sites in third countries

If data processing is carried out in a third country, this is listed in Appendix IV Supplementary Conditions for Order Processing (STC-DP).

6 Evidence to be provided by Telekom

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

☒ compliance with the conventions permitted under Art. 40 GDPR;

☒ certification under a certification procedure in accordance with Art. 42 GDPR

☒ Current certificates, reports or excerpts from reports from independent instances (e.g., auditors, audit department);

☒ a suitable certification (except certificate according to Art. 42 GDPR)

☒ Affidavit by the processor.

Annex III Supplementary Terms and Conditions for Data Processing (STC-DP) for Microsoft Online Services (Office 365/Dynamics 365/Azure)

Technical and organizational measures to provide 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's end. These help 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 enable commissioned data processing in compliance with the agreement even in adverse situations. The processor regularly reviews these for 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 allow for a suitable backup strategy. This particularly takes into account requirements regarding system availability, regular testing of recoverability, and legal requirements concerning storage or erasure.

- **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 privacy 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 specifications. These specifications regulate

  - the use of the applied state of the art of 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 corrections, changes, and deletions by the data subject are made in a timely manner and across all stored records.
  - Storage periods and deletion periods have been defined in accordance with statutory or contractual specifications and are implemented.

c) Confidentiality

- **Commitment of employees**

The employees were committed to maintain data privacy and information protection.

- **Definition and monitoring of the use of permitted resources and communication 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 privacy 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 only in the context of the contractually agreed purpose.

- **Measures for ensuring purpose limitation**

The processor processes personal data exclusively for the contractually agreed purposes and only persons/entities authorized to process data are granted access to this data. The following measures have been taken to avoid chaining of records with different purposes:

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

e) Transparency

- **Directory of procedures**

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

- **Documentation of 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.

- **Ensuring 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.

Annex IV Supplementary Terms and Conditions for Data Processing (STC-DP) for Microsoft Online Services (Office 365/Dynamics 365/Azure)

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

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

1 Approved sub-processors

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

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

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

Deutsche Telekom Individual Solutions & Products GmbH
Friedrich-Ebert-Allee 71-77, 53113 Bonn, Germany
Services: 1st and 2nd level support
Processing site: Germany

Deutsche Telekom Geschäftskunden GmbH
Landgrabenweg 151, 53227 Bonn, Germany
Service: Business customer sales
Processing site: Germany

Deutsche Telekom Privatkunden-Vertrieb GmbH
Landgrabenweg 151, 53227 Bonn, Germany
Service: Business customer sales
Processing site: Germany

Deutsche Telekom IT & Telecommunications Slovakia s.r.o.
Moldavská cesta 8B, 040 11 Košice, Slovakia
Service: Dienstleistungen, Incident Management
Processing site: Slowakei

Deutsche Telekom MMS GmbH
Riesaer Strasse 5, 01129 Dresden, Germany
Services: 1st and 2nd level support
Processing site: Germany

LTIMindtree Limited
Eurocentrum Complex,
Gamma Building - 09th Floor
Al. Jerozolimskie 134
02-305 Warsaw, Poland
Services: 1st and 2nd level support
Processing site: Poland

2 Approved sub-sub-processors

Deutsche Telekom TSI Hungary Kft.
Könyves Kálmán körút 36.
1097 Budapest, Ungarn
Leistung: 1st und 2nd Level Support
Processing site: Ungarn
Used by: Deutsche Telekom MMS GmbH

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.