Supplementary Terms and Conditions for Commissioned Data Processing (Sup-CP) for Cloud of Things

The agreement is entered into between Telekom Deutschland GmbH (hereinafter referred to as Telekom), Landgrabenweg 151, 53227 Bonn, Germany and the customer.

1. General

The subject matter of the agreement is the regulation of the rights and obligations of the controller (customer) and the commissioned processor (Telekom), to the extent that the processing of personal data as part of the service provision (in accordance with the GT&C and other applicable documents) is carried out by Telekom for the customer within the meaning of the applicable data protection laws. The agreement shall apply accordingly to the (remote) testing and maintenance of automated procedures or of data processing systems if, in doing so, the possibility of access to personal data cannot be ruled out. The GT&C and other applicable documents, these "Supplementary Terms and Conditions for Commissioned Processing (Sup-CP)" and the "Annexes to Supplementary Terms and Conditions for Commissioned Processing" (attached Annex) – jointly referred to as "Sup-CP" – provide the legal basis, subject matter, and duration as well as the type and purpose of processing, type of personal data, and the data subject categories. For the use of Cloud of Things, the use of a public cloud called Azure from Microsoft is necessary, as certain hardware and software components are operated there. Insofar as personal data of the customer is processed in this context through the use of the Cloud of Things by the other processor Microsoft Ireland Operations Ltd. and its other processors, Annex 2 (Data Privacy and Security Terms and Conditions for Microsoft Azure Services International) shall apply to this service. In the event of contradictions between the main part of the Sup-CP and Annex 2, Annex 2 shall take precedence for these services.

Definitions

For the purposes of these "Sup-CP" the following definitions apply:

a) The **"processor"** is a natural or legal person, authority, organization, or other agency that processes personal data on behalf of the controller; Telekom is the "processor."

b) **"Third party"** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

c) **"GT&C and other applicable documents"** refer to documents that regulate the provision of services.

d) The **"controller"** is the natural or legal person, authority, organization, or other agency that makes decisions individually or jointly with other parties regarding the purposes and means for processing personal data.

The controller is the contractual party referred to as the "customer" that bears the sole responsibility under these Sup-CP for making decisions regarding the purposes and means for processing personal data.

e) **"Processing"** refers to every procedure performed with or without the aid of automated processes or any series of such procedures relating to personal data such as acquisition, recording, organization, filing, storage, adaptation or modification, reading out, querying, using, disclosing through transmission, dissemination, or any other form of provision, matching, linkage, restriction, deletion, or destruction.

f) **"Personal data"** means any information relating to an identified or identifiable natural person (hereinafter "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of such a natural person.

g) The **"other processor or sub-processor"** refers to the contractual partner of Telekom commissioned by the latter to carry out certain processing activities for the customer, as well as the other processors or sub-processors used by these contractual partners and the other processors or sub-processors used by these processors, etc.

2. Rights and obligations of the customer

2.1 **[Lawfulness of data processing]** The customer shall be solely responsible for assessing whether data can be processed lawfully and for safeguarding the rights of the data subjects. 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.

2.2 **[Instructions]** Telekom shall process personal data only upon the documented instructions of the customer — including the transfer of personal data to a non-EU country or an international organization — unless Telekom is obliged to do so by the law of the European Union or of the member states, to which Telekom is subject. In such a case, Telekom shall notify the customer of such legal requirements prior to the processing, insofar as the relevant law does not prohibit such a notification due to significant public interest.

Instructions are deemed to be the GT&C, other applicable documents, and the Sup-CP. As part of the product-specific parameters, the customer shall determine the nature and scope of the data processing through the type of use of the product, by selecting the options that may be enabled there, e.g., in relation to the scope and type of the data to be processed, or the location of the data processing.

Any and all additional instructions shall be issued in writing or by email. Telekom shall inform the customer immediately if it believes that an instruction violates any applicable legal provisions. Telekom shall be entitled to suspend performance of such an instruction until it is confirmed or changed by the customer.

2.3 **[Settlement for additional services]** Insofar as agreements on service modifications have been entered into in the GT&C and the other applicable documents, such agreements shall take precedence over the provisions in this clause. Insofar as no agreement on service changes has been made in the GT&C and the other applicable documents, additional instructions and measures which constitute a deviation from the services specified in these Sup-CP or in the GT&C and the other applicable documents shall be treated as an application for changes to services. Where additional expenses are incurred beyond these contractually agreed services, Telekom shall be paid separately for additional instructions and measures, unless explicitly agreed otherwise. In this case, the contractual parties shall reach a separate agreement about suitable remuneration. In the event of justified instructions, the implementation of which is not possible for Telekom or only possible with disproportionately high additional expense and therefore cannot be implemented by Telekom, the customer may terminate the agreement without notice.

Unless expressly agreed otherwise, Telekom's support services shall be remunerated separately pursuant to Items 2.5, 3.4, 3.5, 3.7, 3.8 (Sentence 2), 3.9, and 3.10 of this agreement.

2.4 **[Proof from Telekom]** Telekom is entitled to document the adequate implementation of its legal obligations arising from these Sup-CP, in particular the technical and organizational measures (Item 4) and measures that do not only affect the specific commission, with the proofs specified in the Annex.

2.5 **[Checks, inspections]** The customer can audit at its own expense the compliance with the regulations for data protection and the obligations stipulated in these Sup-CP by obtaining information and requesting the proofs listed under Item 2.4 from Telekom with regard to the processing in which it is involved. The customer shall primarily check whether the possibility for inspection granted in Sentence 1 of this paragraph is sufficient. Moreover, the customer may, in exceptional cases to be specially justified, at its own expense, inspect on site the compliance with the data protection regulations. The customer may perform the checks itself or have them performed by a third party it has commissioned at its own expense. Persons or third parties entrusted with such checks by the customer must be obliged in a documented form at the time of commissioning to maintain confidentiality. The persons or third parties entrusted with the checks by the customer shall be announced to Telekom in an appropriate form and enabled to prove their legitimation for carrying out the checks. Third parties in the meaning of this paragraph may not be representatives of Telekom or its Group companies' competitors. The customer shall announce checks within a reasonable period of time and shall take due care during their performance not to disturb business operations.

2.6 **[Support from the customer]** In terms of the processing relating to the customer, the latter shall inform Telekom immediately and in full about any suspicion of data protection infringements and/or other irregularities in the processing of the personal data. In terms of the processing relating to the customer, the latter shall support Telekom promptly and in full in the inspection of possible infringements and in a defense against any claims of affected parties or third parties and in a defense against any sanctions imposed by regulatory authorities.

3. Rights and obligations of Telekom

3.1 **[Data Processing]** Telekom shall process the personal data exclusively in the context of the agreement entered into and under the instructions of the customer in accordance with the provisions under Item 2.2. Telekom shall not use the personal data for any other purposes and shall not pass on the personal data submitted to it to unauthorized third parties. Copies and duplicates must not be created without the prior consent of the customer. This excludes backups required to assure proper data processing.

Telekom guarantees that the employees involved in the processing of the personal data of the customer and other persons operating on behalf of Telekom shall process such personal data only on the basis of the instructions of the customer, unless they are obliged to process the data in accordance with the law of the European Union or the member states.

3.2 **[Data Protection Officer]** Telekom undertakes to appoint an independent, expert and reliable data protection officer, insofar as this is required by the applicable law of the European Union or the member state to which Telekom is subject.

3.3 **[Spatial restrictions; power of attorney]** Telekom shall provide the contractual services in Germany or from the service locations agreed with the customer in the GT&C and other applicable documents as well as the Sup-CDP agreement. The parties shall agree any changes to the location of the data processing if required, in compliance with the form specified in this agreement in accordance with Items 6.2 to 6.6.

Any data processing in non-EU countries (i.e., countries that are not Member States of the European Union and that do not possess an appropriate level of data protection) shall be carried out with due consideration of the relevant, applicable legal provisions of the European Union on the basis set forth in the Annex.

With regard to the standard contractual clauses issued by the European Commission for the transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council, the controller agrees that the processor and/or sub-processor can ensure adherence to Chapter 5 of Regulation (EU) 2016/679 through the use of the standard contractual clauses issued by the European Commission provided that the other prerequisites for the use of the standard contractual clauses are fulfilled.

If the standard contractual clauses cannot be implemented with sub-suppliers in the third country, the regulations in this agreement apply for ensuring legal compliance by Telekom for the deployment of additional sub-processors and for changes [Assistance with controller obligations]. Telekom shall – to the contractually agreed extent, taking into account the nature of the processing and the information available to Telekom – assist the

customer in complying with the obligations imposed on the customer by the applicable, legal provisions.

3.4 **[Support for obligations of the Controller]** Telekom shall – to the contractually agreed extent, taking into account the nature of the processing and the information available to Telekom – support the customer in complying with its obligations imposed on the customer by the applicable, legal provisions.

3.5 **[Support in verification and furnishing requested information]** If the customer is obligated to furnish information on the processing of personal data to a state agency or to a data subject, Telekom shall support the customer in furnishing the said information, provided the said information relates to the data processing under the terms of the agreement, and insofar as the customer is not able to meet the information request itself, or is able to do so merely by selecting specific product parameters.

Depending on the type of processing, Telekom shall support the customer with its obligation to respond to requests for the assertion of the rights of data subjects, if possible with suitable technical and organizational measures. Insofar as a data subject consults Telekom directly with regard to the assertion of their rights, Telekom shall forward the requests of the data subject promptly to the customer.

Telekom shall also notify the customer – insofar as legally permissible – of any communications from the supervisory authorities (e.g., inquiries, notification of measures or requirements) to Telekom in its role as commissioned processor in connection with the processing of personal data under these Sup-CP. Insofar as legally permissible, Telekom shall provide information to third parties, including supervisory authorities, only with the prior written consent of and in coordination with the customer.

3.6 **[Incident reporting]** Telekom shall inform the customer without culpable delay of any incidents of serious disruption to operations, any suspicion of data protection violations, and/or other irregularities in relation to the processing of the personal data.

3.7 **[Proof and documentation]** The parties shall support each other mutually in providing proof and documentation of their due accountability in terms of the principles of proper data processing.

3.8 **[Directory of processing activities performed by commission]** In accordance with the relevant, applicable legal provisions, to which Telekom is subject, Telekom shall maintain a directory of all categories of personal data processing activities commissioned by the customer and performed by Telekom. Telekom shall support the customer on request and shall provide the customer with any details necessary for maintaining its directory of processing activities, insofar as such information lies within the contractually defined scope of responsibility and service of Telekom and insofar as the customer has no other access to this information.

3.9 **[Data protection impact assessment]** If the customer carries out a data protection impact assessment and/or intends to consult the supervisory authority following a data protection impact assessment, the contractual parties shall coordinate the content and scope of any possible support services provided by Telekom, if necessary and on the customer's request.

3.10 **[Completion of the contractual work, return, or deletion]** Personal data that is no longer required, with the exception of personal data that must be retained due to Telekom's legal obligations, must be returned to the customer, unless provisions are already stipulated in the GT&C and the other applicable documents and unless agreed otherwise. The same shall apply to test and waste material. Insofar as it is not already possible for the customer to select certain product parameters accordingly, the customer may, during the existence of the contractual relationship or at the end of the agreement, request in writing, at the customer's expense and in a format agreed in advance, that personal data which has not been destroyed or deleted in accordance with Sentence 1 be surrendered and state a date by when Telekom should surrender the data (at the latest by end of the agreement). A request for a return must be received by Telekom one month prior to the return date specified by the customer and/or one month prior to expiry of the agreement.

4. Technical and organizational security measures

4.1 **[Technical and organizational measures]** The customer and Telekom shall take any suitable technical and organizational measures in order to guarantee a level of protection appropriate to the risk.

Measures that are currently deemed by Telekom to be appropriate are described in the Annex. The customer has evaluated the technical and organizational measures against the background of its specific data processing with regard to an appropriate level of protection and accepted them as appropriate. Any further developments shall be implemented in accordance with Item 4. 2.

4.2 **[Further developments]** The technical and organizational measures may be adjusted to further technical and organizational developments during the course of the contractual relationship. The level of protection must not fall below the agreed level.

The customer shall regularly check the security of the processing and the adequacy of the level of protection and inform Telekom immediately if the technical and organizational measures no longer meet its requirements. The customer shall provide Telekom with all necessary information in this respect. For its part, Telekom regularly monitors the internal processes and the technical and organizational measures to ensure that processing in its area of responsibility complies with the requirements of the EU GDPR and that the rights of the data subject are protected. Where additional expenses are incurred beyond these contractually agreed measures, Telekom shall be paid separately for additional technical and organizational measures, unless explicitly agreed otherwise. In this case, the contractual parties shall reach a separate agreement about suitable remuneration. In the event of instructions being issued that Telekom is not able to implement or only able to implement at disproportionately high additional cost, Telekom shall be entitled to terminate the agreement.

4.3 **[Verification and proof]** Items 2.4 and 2.5 shall apply to the possibilities of verification and proof.

5. Confidentiality

5.1 **[Confidentiality]** Telekom shall maintain the confidentiality of the personal data in relation to the processing agreed in this document. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality, insofar as they are not already subject to an appropriate statutory obligation of confidentiality.

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 concluded 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.

5.2 **[Obligations of persons involved]** Telekom shall familiarize any persons who have access to personal data with the data protection regulations and the provisions of this agreement that are relevant for them.

6. Other processors

6.1 **[Authorization]** Telekom is entitled to deploy further processors in order to perform the tasks described in this agreement.

Commissions that Telekom places with third parties as ancillary services to support the execution of the work assigned to it and that do not involve commissioned processing of personal data for the customer shall not be regarded as a subcontractual relationship within the meaning of this provision.

6.2 **[Special approval]** The customer's approval shall be deemed to have been granted for the other processors listed in the annex and for the areas of responsibility specified therein.

6.3 **[General written approval]** The customer hereby grants Telekom general permission for the future use of other processors.

6.4 **[Information in the event of changes]** Telekom shall inform the customer of any intended change with regard to the involvement of other processors or the replacement of existing processors, whereby the customer shall have the opportunity to object to such changes within 14 days of receipt of the information by the customer. The customer shall not refuse its approval of such changes without a significant reason. If the customer exercises its right of objection and Telekom nevertheless uses the other processor, the customer may terminate the agreement without notice.

6.5 **[Selection]** Telekom shall select other processors who provide sufficient guarantees that the agreed suitable technical and organizational measures will be implemented in such a way that the processing is carried out in accordance with the requirements of the relevant, applicable legal provisions. Telekom shall make contractual agreements with other processors that correspond to the contractual arrangements of these Sup-CP. Telekom shall define the technical and organizational measures with the other processor and have the other processor regularly confirm compliance with the agreed technical and organizational measures. **Notwithstanding the above, the provisions in Annex 2 shall apply to the commissioning of the other processor Microsoft Ireland Operational Ltd. as well as its affiliated companies, with regard to the Microsoft Azure Services.**

6.6 **[Other processors]** The assignment of other processors shall be permissible in accordance with Items 6.1 to 6.5.

7. Changes

1. The following regulations shall apply exclusively and conclusively for changes to the the data processing agreement. They take precedence over other regulations, e.g., regulations established in the main agreement for changes to services, prices, or legal conditions.

1.a) Changes made by the processor

If the processor intends to amend the agreed services or conditions for data processing (e.g., due to decisions by authorities, changes in supplier relationships, legal amendments), they shall inform the controller in writing (e.g., by letter or email) a minimum of 6 weeks before the amendments take effect and prevent any disadvantages for the controller where possible. The amended conditions will become part of the agreement subject to the following requirements:

In the event of amendments which benefit the controller, amendments of minor importance, or binding legal amendments, the processor is entitled to make unilateral amendments to the processing conditions.

For all other amendments, the controller has the right to terminate the services affected when the amendments take effect, without adhering to the notice period. The controller's right of termination shall be expressly referred to in the notification about the amendments.

1.b) Changes made by the controller

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

If the processor agrees to the controller's desired amendments in return for additional remuneration, if applicable, the processor will send them the amended documents. The changes will come into effect at the time stated in the documents if the controller accepts them within 6 weeks.

If the processor rejects the controller's desired amendments or can only deliver them at a significantly higher cost, they shall inform the controller of this. In such a case, the controller is entitled to terminate the service affected without adhering to a notice period.

In the event of a termination, the controller shall be obligated to pay the processor 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 controller can

verify that the damages suffered by the processor were significantly lower or that no damages were suffered at all. The compensation payment shall not be payable provided that the controller has been instructed to suspend the transfer of data by their supervisory authority.

1.c) Continued validity of existing regulations

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

1.d) Suspension

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

8. Term and termination of the agreement

This agreement shall be valid for the duration of the actual provision of services by Telekom. This shall apply regardless of the term of any other agreements (in particular the GT&C and other applicable documents) that the parties have also concluded regarding the provision of the agreed services.

9. Liability and indemnification

9.1 **[Area of responsibility of the customer]** Within its area of responsibility, the customer guarantees the implementation of the obligations arising from the relevant, applicable statutory provisions with regard to the processing of personal data.

9.2 **[Liability]** The liability regulation from the GT&C and the other applicable documents shall apply to these Sup-CP, unless a limitation of liability in accordance with the relevant applicable legal provisions applies in favor of Telekom.

10. Other

10.1 **[Validity of the agreement]** The invalidity of a provision of these 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.

10.2 **[Changes to the agreement]** Any changes to these Sup-CP 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.

10.3 **[General Terms and Conditions]** The parties agree that the "General Terms and Conditions" of the customer shall not apply to these Sup-CP.

10.4 **[Place of jurisdiction]** The sole place of jurisdiction for all disputes arising from and in connection with these Sup-CP shall be Bonn, Germany. This shall apply subject to any sole statutory place of jurisdiction.

10.5 **[Legal basis]** These Sup-CP are based on the provisions of the EU General Data Protection Regulation (EU GDPR). Supplementary country-specific regulations, if any, are listed in the Annex.

10.6 **[Priority regulation]** In the event of contradictions between the provisions of these Sup-CP and the provisions of other agreements, in particular the GT&C and the other applicable documents, the provisions of these Sup-CP shall prevail. In all other respects the provisions of the GT&C and the other applicable documents shall remain unaffected and shall apply to these Sup-CP accordingly.

Annex 1 to the Supplementary Terms and Conditions for Commissioned Processing of Personal Data for Cloud of Things

1. **Details about the Data Processing**

   a. **Information on "Processing Categories":**

   ☒ PaaS (Platform as a Service)

   b. Categories of data subjects:

   ☒ Customers of the controller

   ☒ Employees of the controller

   ☒ Interested parties of the controller

   ☒ Third parties whose data is transferred to the Cloud of Things

   c. Affected 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

   ☒ Personal log data (user names, IP addresses, MAC addresses)

   ☒ All other personal data defined in Article 4 (1) of the GDPR that are transmitted or stored by the customer in the course of the product.

   d. Special types of personal data: (e.g., Article 9 EU General Data Protection Regulation (GDPR)
   None.

2. **Access to personal data**

   The customer shall provide Telekom with the personal data, enable Telekom to access the personal data, or allow Telekom to collect the personal data as described below (as intended, or, in the case of maintenance and support services, as a side effect that cannot be excluded):
   Types of data:

   - Personal data used to authenticate users in the system
   - Configuration settings of user profiles
   - Device data from the respective use case of the controller or third parties

   By default, the customer receives access for an administrator named by it for its tenant. The associated role enables the customer or its administrator to create additional users and assign them authorizations.

   Access for the customer and for third parties to the administration and use of the Cloud of Things is encrypted via the internet using the HTTPS protocol. Each tenant set up for the customer is accessible via an individual URL that is communicated to each user with the transmission of the access data.
   In the event of maintenance and support, the customer shall grant Telekom access to its tenant with the same access rights as the authorizing user. Access is limited in time and can be canceled by the customer at any time.

   ☒ Services in the area of maintenance/remote maintenance/IT fault analysis:

   ☒ Hardware diagnostics via remote access for the following hardware product(s):

   The Cloud of Things has remote maintenance software (VNC) that can be optionally set up for the customer. If this has been done, Telekom has the option of accessing the data of connected machines in the event of maintenance and support.

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

   .....

   Cloud of Things, Push Notification together with the "Cloud of Things" app.

   ☒Approvals for remote maintenance are granted via the help function of the Cloud of Things portal (HTTPS) by an authorized employee of the customer.

   Example: A customer can no longer find its device after it has removed the assignment to an asset.

   The following additional agreements have been reached:

   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.
   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. **Services; purpose of the agreement:**

   The services provided by the processor to the controller are described in the Service Specifications for the Cloud of Things.

4. Processing location:

At the locations of Telekom in Germany and at the locations of the other processors, see Item 7.

5. Technical and organizational security measures

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

a) Confidentiality (Article 32 (1) letter b of the EU General Data Protection Regulation – EU GDPR)

- Admittance control
  No unauthorized access to data processing systems, e.g., magnetic or chip cards, keys, electric door openers, plant security and/or concierge, alarm systems, video systems;
- Access control
  No unauthorized use of the system, e.g., (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data media;
- Data access control
  No unauthorized reading, copying, modifying or removal within the system, e.g., authorization concepts and needs-based access rights, and logging of accesses;
- Separation control
  Separate processing of data that has been collected for different purposes, e.g., multitenancy, sandboxing;

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

- Disclosure control
  No unauthorized reading, copying, modifying or removal during electronic transfers or transport, e.g., encryption, Virtual Private Networks (VPN), electronic signatures;
- Input control
  Definition of whether and by whom personal data was input into, modified or removed from data processing systems, e.g., logging, document management;

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

- Availability control
  Protection against accidental or deliberate destruction and/or loss, e.g., backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), anti-virus protection, firewall, reporting paths and emergency plans;
- Ability to restore availability quickly (Article 32 (1) letter c of the GDPR)

d) Process for regularly testing, assessing, and evaluating (Section 32 (1) Letter d of the EU GDPR; Section 25 (1) of the EU GDPR)

- Data protection management;
- Incident response management;
- Default settings that promote data protection (Section 25(2) of the EU GDPR)
- Commission control
  No commissioned processing within the meaning of Article 28 of the 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.

6. Proof by Telekom

Telekom is entitled to document the adequate implementation of the obligations arising from these Sup-CP, in particular the technical and organizational measures (Item 5) and measures that do not only affect the specific commission, with one of the following proofs:

☒ Compliance with the approved rules of conduct
☒ Certification in accordance with an approved certification procedure
☒ Current certificates, reports, or excerpts from reports from independent instances (e.g., auditors, audit department)
☒ A suitable certification from an IT security or data protection audit
☒ Affidavit by the processor

7. Approved other processors

Details about other processors/services/processing locations

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

Other processors:

1: Deutsche Telekom IoT GmbH, Landgrabenweg 151, 53227 Bonn
Services: General Contractor/Management
Place of production: Germany, Bonn

2: Deutsche Telekom Service GmbH, Friedrich-Ebert-Allee 71-77, Bonn
Services: 1st Level Support
Place of production: Germany, Bonn

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

8. Requirements for commissioned processing in third countries

Commissioned processing in "third countries" is carried out on the basis of the EU standard contractual clauses.

Annex 2 Data Privacy and Security Terms and Conditions for Microsoft Azure Services International

The customer agrees that the provisions of Microsoft's Online Service Terms (https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx?rtc=1) and Microsoft's DPA (https://aka.ms/DPA) apply to its use of Azure Services. The customer is aware that Telekom has entered into a contract with Microsoft based on this provision. The parties agree that in the relationship with Microsoft, only Telekom shall exercise the rights and obligations. There shall be no direct communication between the customer and Microsoft.