Note on commissioned data processing

Should you wish to process personal data in connection with the use of this platform, you must conclude an agreement with T-Systems International GmbH (hereinafter referred to as "T-Systems"), in accordance with the applicable data protection law, regarding the commissioned processing of personal data (CDP). You shall be responsible for checking whether or not the data to be processed is personal data and if the stipulations in the attached Agreement are sufficient according to the applicable data protection law. T-Systems is pleased to provide you with the attached Agreement regarding the processing of personal data.
If you are processing special personal data or other sensitive personal or private data (such as personal data, social data, bank account details, and credit card information, or similar), we recommend that you conclude a specific CDP agreement.
Please send the signed Agreement to the following address:

T-Systems International GmbH
ADV
Dachauer Str. 651
80995 München

T-Systems International GmbH shall sign a copy and send it back to you for your records.

Order for the commissioned processing of personal data

I hereby commission

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt

to process data in accordance with the "Supplementary Terms and Conditions on Commissioned Data Processing" and the "Annex to the Supplementary Terms and Conditions on Commissioned Data Processing."
I understand that the agreement between myself and T-Systems International GmbH shall only be effective under these conditions.

_____
Company

_____
House number and street

_____
Zip code and city

_____
Place, date

_____ _____
Signature Name in block capitals

_____
Place, date (T-Systems International GmbH)

_____ _____
Signature (T-Systems International GmbH) Name in block capitals (T-Systems International GmbH)

Supplementary Terms and Conditions on Commissioned Data Processing in the Open Telekom Cloud

1 General information

The subject matter of the Agreement is the agreement on the rights and obligations of the Customer and T-Systems, to the extent that the collection, processing and use of personal data (hereinafter referred to as "data") as part of the service provision (in accordance with the GT&C and other applicable documents) is carried out by T-Systems for the Customer within the meaning of applicable data protection law. The agreement shall apply accordingly to the (remote) testing and maintenance of automated procedures or of data processing equipment if, in doing so, the possibility of access to personal data cannot be ruled out.

Definitions:

(a) "Personal data" shall mean any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) "Processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) "Controller" or "Customer" shall mean the contractual partner who alone or jointly with others determines the purposes and means of the processing of personal data

(d) "Processor" or "T-Systems" shall mean the contractual partner who processes personal data on behalf of the Controller;

(e) "Third party" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the data;

(f) "The Data Subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. The consent may be revoked at any moment.

2 Responsibility of the Customer and the Customer's right to issue instructions

2.1 As the data controller, the Customer shall be responsible for evaluating the reliability of the collection, processing, and use of the personal data as well as for safeguarding the rights of the data subjects. The Customer shall ensure that the requirements stipulated by law or by authorities are met such as compliance with deletion periods and the permitted storage period, as well as the obtainment of declarations of consent, particularly if the Customer is having especially sensitive data processed

2.2 The Customer shall indemnify T-Systems against all third-party claims vis-à-vis T-Systems within his area of responsibility.

2.3 The Customer shall specify the subject, duration, nature, and purpose of the data processing to take place, if applicable, through his product selection whose service content are specified in the General Terms and Conditions and the other applicable documents and are specified in more detail as regards the data protection requirements in the Annex to the Supplementary Terms and Conditions on Commissioned Data Processing.

2.4 Within 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.

2.5 Additional instructions from the Customer in relation to the processing of personal data that go beyond the contractually agreed services and product parameters and cause T-Systems to incur additional costs, shall be paid for separately. In the event of instructions being issued that T-Systems is not able to implement or is only able to implement at a disproportionately high additional cost, T-Systems shall be entitled to terminate the Agreement. Additional instructions shall be issued in writing.

2.6 The Customer shall inform the Processor regarding the applicable national law and the legal requirements that the Processor needs to know about to perform the data processing in compliance with the respective requirements.

3. T-Systems' obligation of care/the Customer's obligation and right to perform checks

3.1 T-Systems shall process the data exclusively under the terms of the agreements made. T-Systems shall not use the data for other purposes, and, in particular, shall not be entitled to pass on the data submitted to it to third parties. T-Systems shall conduct the necessary technical and organizational measures which are required for the protection of the data and which are specified in the Annex to the Supplementary Terms and Conditions for Commissioned Data Processing. Within the scope of these specifications, T-Systems may adapt the technical and organizational measures based on its own professional judgment of the technical and organizational developments.

3.2 T-Systems shall provide suitable certificates with which the Customer can monitor compliance with the provisions on data protection as regards the data processing that concerns him. They shall be provided to the Customer on request and shall be updated at regular intervals, no less than every 24 months. The Customer may carry out individual checks in particularly exceptional cases, stating the reasons for this. These checks may be carried out by the Customer himself at his expense or by a third party commissioned by him. It shall be documented at the time of commissioning that the third party is obligated to maintain confidentiality. Third parties within the

meaning of this agreement may not be representatives of T-Systems' competitors. The Customer shall announce individual checks with a reasonable period of notice and shall take due care during their performance not to disturb business operations and operational processes. The Customer shall reimburse T-Systems separately for any additional costs incurred by T-Systems as a result of such checks.

4 Other rights and obligations of the Customer and of T-Systems

4.1 The Customer shall be responsible for complying with the rights of the data subjects, such as the correction, deletion, and blocking of access to data, which may be asserted against him. Through the usage options of the product parameters, T-Systems shall provide that the Customer can comply with the rights of the data subjects. If a data subject asserts its right to the correction, deletion or blocking of access to data against the Customer and if the Customer is not able to comply with the right through not having the corresponding choice of particular product parameters, T-Systems shall, in consultation with the Customer, carry out the correction, blocking of access to or the deletion of the data, provided that it is legally and actually possible for it to do so.

4.2. Documents with personal data and files that are no longer needed shall be destroyed in accordance with the contractual agreement and data protection provisions, with the exception of data that must be retained by T-Systems under its statutory obligations. The same shall apply to testing and waste material. If the storage media is in the possession of the Customer, the Customer shall delete all personal data in compliance with data protection provisions before handing the storage media over to T-Systems or its subcontractors. If this is not possible for the Customer, he shall inform T-Systems in good time in writing. T-Systems shall then be entitled to delete personal data on behalf of the Customer. Where not expressly agreed, the cost for deletion shall be reimbursed separately.

4.3 At any time during the term of the Agreement or up to three months thereafter, the Customer may submit a written request for the return of the data that was not deleted pursuant to Item 4.2. After expiry of this period, T-Systems shall delete any remaining data with the exception of data that must be retained to satisfy T-Systems' statutory obligations. The request for the return of the data must be received by T-Systems one month before expiry of the period. The data may also be returned after the period has expired

4.4 T-Systems shall inform the Customer if it considers data processing activities to be violating data protection provisions. T-Systems shall be entitled to suspend performance of the relevant data processing activities until the Customer either confirms these activities to be compliant with data protection provisions or changes them.

4.5 T-Systems shall inform the Customer of any cases of serious disruptions to operations, any suspicion of data protection violations, infringements of the stipulations made in this Agreement, and other significant irregularities in the processing of the Customer's data.

4.6 T-Systems has appointed a competent and reliable in-house data protection officer, who shall be granted the time required to carry out his or her duties.

4.7 If the Customer is obligated to provide information about the processing of data to a government agency or an individual, T-Systems shall support the Customer in submitting this information. Unless otherwise expressly agreed, the cost for such support services shall be reimbursed to T-Systems separately.

5. Testing, maintenance, remote access

5.1 To the extent that access to personal data cannot be ruled out during test and maintenance work of automatic procedures or data processing equipment, including those as part of remote access, T-Systems shall make use of the access only to the extent, and within the time frame, that is absolutely necessary to properly perform the contracted maintenance and test work.

5.2 T-Systems' employees shall use reasonable identification and encryption procedures. Where not otherwise expressly agreed, each party shall be responsible for all data backup measures in its respective area of responsibility.

5.3 All testing and maintenance work, including that performed by remote access, shall be documented and logged.

6. Data processing abroad

6.1 T-Systems shall provide the contractual services in Germany or from the service locations agreed with the Customer. If T-Systems wishes to provide all or part of the services due from a different location abroad, T-Systems shall obtain consent from the Customer in accordance with the procedure for <Changes in General Terms and Conditions, Service Specifications and Prices>.

6.2 The Customer shall not unreasonably refuse his consent to the relocation of service provision from Germany to another country. T-Systems shall document the specific sites of service provision and provide evidence to the Customer upon request.

6.3 If data processing work is permitted outside Germany pursuant to this Agreement and to the statutory requirements for the commissioned processing of personal data or for transmitting personal data to other countries, T-Systems shall provide compliance with and implementation of the statutory requirements when exchanging data across borders.

7. Subcontractors

7.1 T-Systems may use subcontractors to perform the tasks described herein. If T-Systems uses subcontractors as part of its service provision, it shall list them in the Annex to the Supplementary Terms and Conditions on Commissioned Data Processing for the Open Telekom Cloud.

7.2 If T-Systems decides to change subcontractors, it shall obtain consent from the Customer in accordance with the procedure for <Changes to the General Terms and Conditions (GT&C) and the Service Specifications and prices>.

7.3 T-Systems shall make contractual agreements with subcontractors which correspond to the contractual arrangements of this agreement. When commissioning subcontractors outside Germany, T-Systems shall, within its area of responsibility, observe any legal provisions for the commissioned processing of personal data or for transmitting personal data to other countries as well as the provisions in § 6 (6.1) to (6.4).

8. Other points

8.1 The invalidity of a provision of this Agreement shall not affect the validity of the remaining provisions. If a provision proves to be invalid, T-Systems shall replace it with a new provision that approximates as closely as possible to the intentions of the Customer and T-Systems.

8.2 In the event of contradictions between the provisions of this Agreement and the provisions of other agreements, the provisions of this Agreement and the Annex to the Supplementary Terms and Conditions for Commissioned Data Processing shall take precedence.

Annex to the Supplementary Terms and Conditions on Commissioned Data Processing in the Open Telekom Cloud

1 General information

1.1 The Customer and T-Systems have agreed on the validity of the Supplementary Terms and Conditions on Commissioned Data Processing.

1.2 The parties hereby agree the following specific details based on the General Terms and Conditions, the related Service Specifications or other documents, as well as the Supplementary Terms and Conditions on Commissioned Data Processing.

2. Scope, nature, and purpose of the intended collection, processing, or use of data

2.1 The subject matter, scope, nature, and purpose of the collection, processing, and/or use of personal data by T-Systems for the Customer are specified in the General Terms and Conditions or service agreements, as well as the specific product parameters, as well as their use by the Customer.

2.2 Type of data

The following types/categories of data (listing/ description of data categories) may be the subject matter of the collection, processing and/or use of personal data:

- Name
- Contact data (e.g., telephone, e-mail)
- Data that can be traced back to individuals or personal log data (user names, IP address)
- Access Information
- Consumption Information

2.3 Group of data subjects

The group of data subjects, whose data is used as part of this order, may include the following categories of individuals:

- Customers
- Employee

3. Data processing locations and subcontractors

3.1 Service provider (country, address, brief description of the service)

Name of service provider	Country	Address	Brief description of the service
T-Systems International GmbH	Germany	Hahnstr., 43d, 60528 Frankfurt	Processor
Deutsche Telekom Regional Services and Solutions GmbH	Germany	Friedrich-Ebert-Allee 71 -77, 53113 Bonn	1st Level Support
IT Services Hungary	Hungary	H-1117 Budapest, Neumann Janos u 1/C	Operation, 2nd Level Support
STRATO AG	Germany	10587 Berlin, Pascalstrasse 10	Service Desk
Axivas Deutschland GmbH	Germany	68723 Schwetzingen, Carl-Benz-Straße 9-11	Service Desk

4. Procedure for deleting/destroying personal data in accordance with data protection provisions

If T-Systems is legally or contractually obligated to delete/destroy personal data, the parties shall agree the following procedures for deletion/destruction in compliance with agreements:

4.1. Erasing hard disks, USB sticks, rewritable data media

- Data media are to be replaced or destroyed in accordance with the procedures outlined by the procurement and disposal processes.
- Data media must be disposed of in line with the information protection policy or the Customer order.
- The deletion or destruction of data media must be logged.

In addition, the following points must be observed:

- The deletion of data always extends to any back-up that might be present.
- Data deletion must be logged.

4. 2 Deletion of files on hard disks, USB sticks, and other rewritable data media

The data media in question are to be fully deleted using one of the suitable methods listed under Item 4.1. However, where only individual files are to be deleted in accordance with data protection regulations, the software used must overwrite the file to be deleted, not merely delete its directory entry.

The following methods are not suitable:

- Deletion using the Delete key
- Moving the file to the recycle bin
- Renaming the file

5. Technical organizational measures

5.1 Admittance control

The aim of admittance control is to deny unauthorized persons access to data processing equipment that processes or uses personal data.
The following admittance controls are in place:

1) Definition of security areas
2) Management and documentation of individual admittance authorizations throughout the entire life cycle
3) Accompanying visitors and external personnel
4) Monitoring rooms outside of business hours
5) Logging access to the data-processing
1) IT-systems

5.2 System access control

The aim of system access control is to prevent unauthorized persons from using data processing systems that process or use personal data.
The following system access control measures are in place:

1) Access protection (authentication)
2) Strong authentication for maximum level of protection
3) Simple employee authentication (with user name/password) for high level of protection
4) Secure transmission of authentication credentials within the network
5) Individuals with access authorization are explicitly defined and restricted to a minimum
6) Personal authentication media are documented and administrated
7) Successful and rejected access attempts are logged
8) Specification of authorized individuals
9) Automatic and manual blocking of access when an individual leaves his post

5.3 Data access control

Data access control measures must ensure that only data for which a person is authorized can be accessed, and that personal data cannot be read, copied, changed, or deleted by unauthorized persons during processing, use, or after saving.
The following admittance controls are in place:

1) Creation of an authorization concept
2) Implementation of access restrictions
3) Assignment of minimum authorizations
4) Personal access authorizations are administrated and documented
5) Data access logging

5.4 Disclosure control

The aim of disclosure control is to ensure that personal data cannot be read, copied, changed, or deleted by unauthorized persons during electronic transmission or during transport, or be saved on data media, and that it is possible to check and determine where personal data is to be transmitted to by means of data communication equipment.
The following disclosure control measures are in place:

1) Logging of every transmission or a representative selection of transmissions
2) Secure server-client data transmission
3) Safeguarding transmission in the back end
4) Security gateways at the network transfer points
5) Deletion of preset service accounts/passwords and non-required services
6) Description of all interfaces and the transmitted personal data fields
7) Every machine included in the IT process has its own unique ID/password
8) Data storage is performed exclusively on the platform and the back-up systems
9) The complete and permanent deletion/erasure of data and data media containing Customer data of the Customer in compliance with data protection rules is logged

5. 5 Input control

The aim of data input control is to ensure by means of suitable measures that the details of data input can be checked and ascertained subsequently.
The following input control measures are in place:

1) Logging of data inputs

5.6 Job control

The aim of job control is to ensure that in the case of commissioned processing of personal data, the data is processed strictly in accordance with the Customer's instructions.
The following job control measures are in place:

1) Provisions/restrictions for executing orders

5.7 Availability control

The aim of availability control is to ensure that personal data is protected against accidental destruction or loss.

The measures for availability control are set out in the "Service Specifications „Service Description Open Telekom Cloud" in sections 2.2 Storage, 2.2.3 Volume Backup Service and 2.9 Disaster Recovery.

5.8 Intended use control

The aim of intended use control is to ensure that data collected for different purposes can be processed separately.
The following intended use control measures are in place:

1) Economy in data collection
2) Separate processing and/or storage of data with different contractual purposes.

6. Approved subcontractors name, address, headquarters and any relevant different secondary office

Name of subcontractor	Address of headquarters/secondary office (if applicable)	
Deutsche Telekom Regional Services and Solutions GmbH	Germany	Friedrich-Ebert-Allee 71 -77, 53113 Bonn	1st Level Support
IT Services Hungary	Hungary	H-1117 Budapest, Neumann Janos u 1/C	
STRATO AG	Germany	10587 Berlin, Pascalstrasse 10	Service Desk
Axivas Deutschland GmbH	Germany	68723 Schwetzingen, Carl-Benz-Straße 9-11	Service Desk