



# Purchasing conditions of the Deutsche Telekom Group relating to commissioned processing of personal data (PC CDPA Europe)

## 1. Subject matter of these Terms and Conditions; legal basis

- (1) The Controller (i.e., the Customer) intends to commission the Processor (i.e., the Contractor) with the provision of services in the context of the service relationship (hereinafter referred to as "Framework Agreement") based on individual orders/call orders (hereinafter referred to as "Individual Agreement"). If, in this context, the Processor processes personal data (hereinafter also referred to as "Data"), or insofar as access to personal data cannot be excluded (in particular when services in the area of maintenance/remote maintenance/IT fault analysis are performed), these activities shall be governed by
- the present Purchasing Conditions of the Deutsche Telekom Group relating to the processing of Personal Data on behalf of a Controller (hereinafter also referred to as the "Terms of Purchase") and
  - the terms and conditions of every additional Individual Agreement on the commissioned processing of personal data on behalf of a Controller (hereinafter referred to as "Individual CDPA") that is to be concluded along with every Individual Agreement.

In the event of any inconsistencies between these Terms of Purchase and the provisions of an Individual CDPA, the provisions of these Terms of Purchase shall take precedence. Anything to the contrary shall only apply if the Parties have expressly agreed to a deviation from these Terms of Purchase in the Individual CDPA by specifically stating and referring to the provision of these Terms of Purchase which is intended for amendment.

- (2) The Customer within the meaning of this Terms of Purchase is Deutsche Telekom AG (DTAG) or an affiliated company of DTAG within the meaning of the Framework Agreement.
- (3) The Customer and the Contractor agree on the Standard Contractual Clauses (hereinafter referred to as „Clauses“ or “SCC”) between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament with the clarifications and additions set forth in the following Annexes I - V. These clauses are listed in cipher 2. To the extent that the Clauses refer to the applicability of provisions of either Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, the reference to Regulation (EU) 2016/679 shall apply in each case. An amendment of the clauses is not permitted.

## 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 [choose relevant option: OPTION 1: 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, and repealing Directive 95/46/EC (General Data Protection Regulation)] / [OPTION 2: Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC].
- 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) of 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(s)**

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**

**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 sub-processors

a) OPTION 1: PRIOR SPECIFIC AUTHORISATION: The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION: 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 [SPECIFY TIME PERIOD] 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.

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 [OPTION 1] Article 32 of Regulation (EU) 2016/679/ [OPTION 2] Articles 33 and 36 to 38 of Regulation (EU) 2018/1725

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 of Regulation (EU) 2016/679 or under Articles 34 and 35 of 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 [OPTION 1] Article 33(3) of Regulation (EU) 2016/679/ [OPTION 2] Article 34(3) of Regulation (EU) 2018/1725, 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 [OPTION 1] Article 34 of Regulation (EU) 2016/679 / [OPTION 2] Article 35 of Regulation (EU) 2018/1725, 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 [OPTION 1] Articles 33 and 34 of Regulation (EU) 2016/679 / [OPTION 2] Articles 34 and 35 of Regulation (EU) 2018/1725.

### 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.

## **ANNEX I**

### **Purchasing conditions of the Deutsche Telekom Group relating to commissioned processing of personal data (PC CDPA Europe)**

#### **LIST OF PARTIES**

Parties are the contractual partners of the Individual CDPA.

## **ANNEX II**

### **Purchasing conditions of the Deutsche Telekom Group relating to commissioned processing of personal data (PC CDPA Europe)**

#### **DESCRIPTION OF PROCESSING**

Processing is described in the Individual CDPA.

## **ANNEX III**

### **Purchasing conditions of the Deutsche Telekom Group relating to commissioned processing of personal data (PC CDPA Europe)**

#### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The following measures are agreed:

Case variant 1:

- The processor uses his own (or a sub-processor's) IT infrastructure (server/client, application) or his own end devices, either exclusively or in addition. Or:
- The processor or a sub-processor stores personal data of the controller in his own IT infrastructure or in his own end devices

The following measures apply: TOM1

OR

Case variant 2

- The processor uses the controller's IT infrastructure (server/client, application) and uses his own (or a sub-processor's) end devices to access it. No data is stored by the processor or a third party

The following measures apply: TOM2

OR

Case variant 3

- The processor uses only the IT infrastructure (server/client, application) and end devices of the controller.

The following measures apply: TOM3

## **ANNEX IV**

### **Purchasing conditions of the Deutsche Telekom Group relating to commissioned processing of personal data (PC CDPA Europe)**

#### **LIST OF SUB-PROCESSORS (INCL. SUB-SUB-PROCESSORS)**

Sub-processors and the authorisation procedure to the use of additional sub-processors and sub- sub-processors (option pursuant to clause 7.7 are listed in the Individual CDPA.

## **ANNEX V**

### **Purchasing conditions of the Deutsche Telekom Group relating to commissioned processing of personal data (PC CDPA Europe)**

#### **ADDITIONAL AGREEMENTS**

1. **Telecommunication Secrecy**  
If, in the scope of its activities, it is possible for the processor to access electronic communications data, it shall guarantee that the confidentiality obligation on the persons entrusted with the processing extends to the content and precise circumstances of the electronic communication of the data subject, in particular the involvement of the data subject in an electronic communication process and the precise circumstances of failed communication attempts.
2. **Controller's direct audit right**  
In the event that the controller processes the personal data covered by this contract on behalf of a superordinate customer, i.e., if the Data to be processed is personal data of a client of the controller, the processor shall also, on request of the superordinate customer, extend the granting of information and monitoring rights to this superordinate customer. In this case the processor shall continually provide the controller with details on the information given and checks carried out in writing or by e-mail.
3. **Quality assurance**  
If the processor gets access to controller's data processing systems the following is pointed out: The controller reserves the right to perform quality assurance audits and to take measures to identify misuse of such systems (e.g. Logs). This may include accessing the personal data (such as but not limited to individual user IDs and names, contact information, etc.) of those employees of the processor who have access to the systems.
4. **Insofar as services are provided in the area of maintenance, remote maintenance and/or IT fault analysis the following supplementary regulations shall apply:**
  - a. The employees of the processor shall use appropriate identification and encryption procedures. Before the work is carried out, the controller and the

- processor shall agree on any necessary data backup measures.
- b. All services shall be documented and logged by the processor
  - c. The data may only be used at the explicit request of the controller and only for fault analysis purposes. They may only be used on the equipment provided by the controller or on the processor's equipment that has been previously approved by the controller for this purpose. The data may not be copied to mobile storage media (PDAs, USB memory sticks or similar devices) without the explicit consent of the controller.
  - d. Testing and maintenance work on workstation systems at the controller shall be carried out upon approval by the relevant authorized individual/affected employee of the controller.
  - e. The processor shall make use of the access rights granted to it - also in terms of time - as necessary for the proper performance of the commissioned maintenance and testing work.
  - f. In the case of remote access, the controller shall be entitled - insofar as technically possible - to monitor such access from a control screen. Insofar as the functionality "Termination of remote access by the controller" is necessary, the contracting parties shall agree on the establishment of this functionality and further modalities.
5. Sub-processors  
The obligations pursuant to this Annex V must also be imposed on the sub-processor by the processor accordingly.
  6. Encryption  
Data (including any personal data therein) in transit over public networks between data exporter and data importer, or between data importer's data centers, must be encrypted by the data importer by default. Data importer also encrypts data stored at rest in its systems including its cloud environment
  7. Backdoors  
The data importer certifies that (1) it has not purposefully created back doors or similar programming that could be used to access the system and/or data (2) it has not purposefully created or changed its business processes in a manner that facilitates access to data or systems, and (3) that national law or government policy does not require the data importer and/or its sub-processors to create or maintain back doors or to facilitate access to data or systems or for the data importer and/or its sub-processors to be in possession or to hand over the encryption key.
  8. International data transfers  
With regard to clause 7.8 b of the Clauses, the processor is aware that a prerequisite for the applicability of the standard contractual clauses adopted by the Commission pursuant to Article 46(2) of Regulation (EU) 2016/679 is a positive outcome of a risk assessment to be carried out by the processor of the partner processing data in the third country or having access to the data from the third country. The result and the main underlying considerations of the risk assessment shall be documented and proven/submitted to the controller upon request.
  9. Cooperation with supervisory authorities  
In addition to clause 7.6 e, the processor shall promptly inform the controller - subject to mandatory legal requirements - of all notifications of the supervisory authorities (e.g. requests, notification of measures or requirements) addressed to the processor or the sub-processor in connection with the processing of data under this agreement
  10. Docking clause  
Clause 5 (Docking clause) of the Standard Contractual Clauses shall apply.
  11. Separate instructions of controller (if applicable) are listed in der Individual CDPA.