

# MindSphere Data Privacy Terms

October 2022

## 1. Purpose, scope and term

1.1. The Data Privacy Terms (“DPT”) constitute a data processing agreement between you and us and shall apply to all Services that involve the Processing of Personal Data by us acting as Processor or Subprocessor for you.

1.2. The DPT describe our and your data protection related rights and obligations with regard to the Services captured by this DPT. All other rights and obligations shall be exclusively governed by the other parts of the MindSphere Agreement.

1.3. You shall ensure (also in relation to your Authorized Entities) that we and our Subprocessors are allowed to provide the Processing Services as Processor and Subprocessor as described in this DPT.

1.4. Certain capitalized terms used in this DPT are defined in Section 11. Other capitalized terms shall have the meaning given to them in this document, or elsewhere in the MindSphere Agreement.

## 2. Details of the Processing Services provided by us

2.1. The details of the Processing Services provided by us, including the scope, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of affected Data Subjects, are specified in [Attachment 1](#) to this DPT.

2.2. We will Process Personal Data in accordance with the terms of the MindSphere Agreement (including the terms of this DPT) or as otherwise permitted by you.

2.3. We shall be entitled to disclose or to entitle our Subprocessors to disclose Personal Data to comply with Laws and/or governmental orders. In case of such a request, we or the Subprocessor will (i) use reasonable efforts to redirect such requesting entity to request data directly from you and may provide your basic contact information, and (ii) promptly notify you and provide a copy of the request, unless we are prevented from doing so by Laws or governmental order.

## 3. Instruction rights

3.1. As Processor, we will only act upon your documented instructions. The MindSphere Agreement (including the DPT) constitutes your complete and final instructions for the Processing of Personal Data by us as your Processor.

3.2. Any additional or alternate instructions must be agreed between you and us in writing and may be subject to additional costs.

3.3. We shall inform you if, in our opinion, an instruction infringes Applicable Data Protection Law. We shall, however, not be obligated to perform any legal examination of your instructions.

## 4. Technical and organizational measures

We will implement the technical and organizational measures described in [Attachment 2](#) to this DPT. You hereby confirm that the level of security provided is appropriate to the risk inherent with the

Processing by us on your behalf. You understand and agree that the technical and organizational measures are subject to technical progress and development. In that regard, we shall have the right to implement adequate alternative measures as long as the security level of the measures is maintained.

## 5. Confidentiality of the Processing

We will ensure that personnel who are involved with the Processing of Personal Data under the DPT have committed themselves to confidentiality.

## 6. Subprocessors

Subject to Applicable Data Protection Law, you hereby approve the engagement of Subprocessors by us. You understand that to the extend the Processing of Personal Data is necessary for the Subprocessors to provide the Service, the Subprocessors may access such Personal Data. In case of any commissioning of Subprocessors, we shall, where required by Applicable Data Protection Law, enter into an agreement with such Subprocessor imposing appropriate contractual obligations on the Subprocessor that are no less protective than the obligations in this DPT. We remain responsible for any acts or omissions of our Subprocessors in the same manner as for our own acts and omissions hereunder.

## 7. Rectification and erasure

7.1. We shall, at our discretion, either (i) provide you with the ability to rectify or delete Personal Data via the functionalities of the Services, or (ii) rectify or delete Personal Data as instructed by you. If this requires your or your Authorized Entities support, you shall provide all necessary support and procure the support of the respective Authorized Entity in order for us to fulfill this obligation.

7.2. After termination of a Service, we will delete or anonymize your Personal Data that is associated with such Service from the Platform in accordance with the terms of the MindSphere Agreement, unless we are required to retain such data in accordance with Laws. You acknowledge that part of your Personal Data may be retained by us as part of our disaster recovery backup of the Platform until deletion of such files in accordance with our policies.

## 8. Personal Data Breach

In the event of any Personal Data Breach, we shall notify you of such breach without undue delay after we become aware of it. We shall (i) reasonably cooperate with you in the investigation of such event; (ii) provide reasonable support in assisting you in your security breach notification obligations under Applicable Data Protection Law (if applicable); and (iii) initiate respective and reasonable remedy measures.

## 9. Further notifications

We shall notify you without undue delay of (i) complaints or requests of Data Subjects whose Personal Data are Processed pursuant to this DPT (e.g. regarding the rectification, erasure and restrictions of Processing of Personal Data) or (ii) orders or requests

by a competent data protection authority or court which relate to the Processing of Personal Data under this DPT unless we are prevented from doing so by the Law or governmental order.

#### 10. **Effective date of the DPT**

The DPT shall come into effect upon your signing or upon your use of any Service.

#### 11. **Definitions**

11.1. **“Applicable Data Protection Law”** means all applicable law pertaining to the Processing of Personal Data hereunder.

11.2. **“Authorized Entities”** means (i) your Affiliates and (ii) other legal entities entitled to access and use the Services or employing Users entitled to access and use the Services via your designated Account.

11.3. **“Controller”** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

11.4. **“Data Subject”** means an identified or identifiable natural person.

11.5. **“DPT”** shall mean this Data Privacy Terms.

11.6. **“Emergency Replacement”** refers to a short-term replacement of a Subprocessor which is necessary (i) due to an event outside of our reasonable control and (ii) in order to provide the Services without interruptions (such as if the Subprocessor unexpectedly ceases business, abruptly discontinues providing services to us, or breaches its contractual duties owed to us).

11.7. **“Personal Data”** means information that relates, directly or indirectly, to a Data Subject, including without limitation, names, email addresses, postal addresses, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Data, for the purposes of this DPT, includes only such Personal Data entered by you or any Authorized Entity into or derived from the use of the Services; i.e. Personal Data is a sub-set of Your Content and used herein when any Data Protection Law applies.

11.8. **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed under the terms of this DPT.

11.9. **“Processor”** means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Controller.

11.10. **“Process”** or **“Processing”** means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or

combination, restriction, erasure or destruction, access to, transfer, and disposal.

11.11. **“Subprocessor”** shall mean any further Processor engaged by us in the performance of the Services provided under the terms of this DPT that has access to Personal Data.

11.12. **“Special Categories of Personal Data”** shall mean information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, social security measures, administrative or criminal proceedings and sanctions, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

## ATTACHMENT 1 TO THE DPT

The Parties may provide further details in the Order Forms if required for a particular Service, or we may provide further details in the applicable Transaction Documents.

### **Processing operations**

We and our Subprocessors will Process Personal Data as follows:

- to provide the Services
- to provide storage and backup of Personal Data in data centers in connection with providing the Services (multi-tenant architecture)

### **Data Subjects**

The Personal Data Processed concerns the following categories of Data Subjects:

Data Subjects include employees, contractors, business partners or other individuals whose Personal Data is stored on the Platform.

### **Categories of data**

The Personal Data Processed concerns the following categories of personal data:

You, your Authorized Entities and Users determine the categories of Personal Data that will be Processed in connection with the Services. The respective data fields can be configured as part of the implementation of the Service or as otherwise permitted in the Service. The Personal Data Processed may include: name, phone number, email address, time zone, address data, system access / usage / authorization data, company name, contract data, invoice data, and any application-specific data which Users enter into the Service including bank account data, credit or debit card data.

### **Special Categories of Personal Data (if appropriate)**

The Services are not intended for the processing of Special Categories of Personal Data and you and your Authorized Entities shall not transfer, directly or indirectly, any such sensitive personal data to us.

ATTACHMENT 2 TO THE DPT

Some Services may be protected by different or additional technical and organizational security measures (TOMs), as set forth in the respective Order Forms or the applicable Transaction Documents. In all other cases, we shall implement and maintain appropriate technical and organizational measures as described at <https://www.alibabacloud.com/trust-center>.

# MindSphere Additional European Terms – Part 1

October, 2022

## 1. Purpose and scope

- 1.1 These Additional European Terms apply only if and to the extent an Authorized Entity is located in the European economic Area or Switzerland. The Additional European Terms incorporate the body document of the DPT (including [Attachment 1](#) and [Attachment 2](#)) by reference.
- 1.2 The Additional European Terms also include the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 (“**EU Model Contract**”). We enter into the EU Model Contract in our role as data importer, you enter into the EU Model Contract in your role as data exporter. The EU Model Contract is contained in Part 2 of the Additional European Terms. If and to the extent there should be contradictions or inconsistencies between Part 1 and Part 2, the provisions of Part 2 shall prevail. For the avoidance of doubt, provisions in Part 1 that merely go beyond Part 2 (i.e., the terms of the Model Contract) without contradicting Part 2, shall remain valid.
- 1.3 If a direct contractual relationship (including the EU Model Contract) between us and the respective Authorized Entity is mandatory under Applicable Data Protection Law, the respective Authorized Entity shall have the right to accede by unilateral declaration to the Additional European Terms (including the EU Model Contract) having the rights and obligations assigned to you therein (unless the rights and obligations are explicitly granted exclusively to the customer that entered into an MMA with us (“**MMA Party**”). We hereby waive the need to be notified of the declaration of accession by an Authorized Entity, i.e. the Authorized entity shall be a party to the Additional European Terms as soon as the Authorized Entity declared its accession (and regardless of the declaration being received by us). In case an Authorized Entity accedes to these Additional European Terms, the MMA Party shall serve as a single point of contact for us with regard to Authorized Entities and its Users. The rights granted to Authorized Entities herein (and any related liability claims) shall be exercised by the MMA Party vis-à-vis us and shall be subject to limitations of liability agreed in the MindSphere Agreement. We are entitled to refuse any requests, instructions or claims provided directly by an Authorized Entity other than the MMA Party. We shall be discharged of our obligation to inform or notify an Authorized Entity when we have provided such information or notice to the MMA Party.

## 2. Further support

At your request, we shall reasonably support you in (i) fulfilling your obligation to respond to requests for exercising Data Subject's rights or (ii) fulfilling any of your further obligations as Controller under

Applicable Data Protection Law (such as the obligation to conduct a data protection impact assessment). Such support shall be compensated by you on a time and material basis.

## 3. Subprocessors

- 3.1 You hereby approve the engagement of Subprocessors by us. A current list of Subprocessors commissioned by us can be found at [https://help.aliyun.com/document\\_detail/123950.html](https://help.aliyun.com/document_detail/123950.html).
- 3.2 We agree and understand that Applicable Data Protection Law in the EEA requires a Processor (i) not to engage another Processor without prior specific or general authorization and, (ii) in case of a general authorization, to give the Controller the opportunity to object to changes to the Subprocessors used. Such right to object of Authorized Entities shall be exclusively governed by the contractual relationship between MMA Party and the respective Authorized Entity.
- 3.3 Between MMA Party and us the right to object shall apply as follows: we may remove or add new Subprocessors at any time. We will obtain MMA Party's approval (on its own behalf and on behalf of Authorized Entities) to engage new Subprocessors in accordance with the following process: (i) we shall publish new Subprocessors at [https://help.aliyun.com/document\\_detail/123950.html](https://help.aliyun.com/document_detail/123950.html) at least twenty (20) days before authorizing any new Subprocessor to access Personal Data Processed hereunder; new Subprocessors shall be published on the 15th of each calendar month; (ii) if MMA Party raises no reasonable objections (on its own behalf or on behalf of Authorized Entities) that include an explanation of the grounds for non-approval in writing within this 20 day period, then this shall be taken as an approval of the new Subprocessor; (iii) if MMA Party raises reasonable objections (on its own behalf or on behalf of Authorized Entities), we will - before authorizing the Subprocessor to access Personal Data Processed hereunder - use reasonable efforts to (a) recommend a change to the configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor or (b) propose other measures that address the concerns raised in the objection; (iv) if the proposed changes or measures cannot eliminate the grounds for non-approval, MMA Party may terminate the affected Service with 10 days' notice following our response to its objection.
- 3.4 We shall be entitled to perform Emergency Replacements of Subprocessors. In such a case, if required by Applicable Data Protection Law, we shall inform you of the Emergency Replacement without undue delay and the approval process as described in Section 3.2 shall apply after your receipt of the notification.

#### 4. Audits

- 4.1 You shall have the right to audit, by appropriate means - in accordance with Sections 4.2 to 4.5 below - our and our Subprocessors' compliance with the data protection obligations hereunder annually (in particular in regard to the technical and organizational measures we implement), unless additional audits are necessary under Applicable Data Protection Law; such audit being limited to information and data processing systems that are relevant for the provision of the Services provided to you.
- 4.2 We and our Subprocessors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder, especially the requirement to implement technical and organizational measures in accordance with Section 4 of the DPT. Each audit will result in the generation of an audit report (e.g. as Service Organization Controls 1, Type 2 reports and Service Organization Controls 2, Type 2 reports). Where a control standard and framework implemented by us or our Subprocessors provides for audits, such audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- 4.3 You agree that these audit reports and corresponding information provided by us (together "**Audit Reports**") shall first be used to address your audit rights under this DPT. Upon your request, we shall provide such relevant Audit Reports for the Services concerned.
- 4.4 In case you can demonstrate that the Audit Reports provided are not reasonably sufficient to allow you or an Authorized Entity to comply with applicable audit requirements and obligations under Applicable Data Protection Law, you or the respective Authorized Entity shall specify the further information, documentation or support required. We shall render such information, documentation or support within a reasonable period of time at your expense.
- 4.5 The Audit Reports and any further information and documentation provided during an audit shall constitute Confidential Information and may only be provided to Authorized Entities pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the MindSphere Agreement. In case audits relate to our Subprocessors, we may require you and Authorized Entities to enter into non-disclosure agreements directly with the respective Subprocessor before issuing Audit Reports and any further information or documentation available to you or Authorized Entities.

# MindSphere Additional European Terms – Part 2

## Standard Contractual Clauses for Processors

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

### Clause 1

#### Definitions

For the purposes of the Clauses:

- (a) “personal data”, “special categories of data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority” shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) “the data exporter” means the controller who transfers the personal data;
- (c) “the data importer” means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) “the sub-processor” means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) “the applicable data protection law” means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) “technical and organisational security measures” means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

### Clause 2

#### Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

### Clause 3

#### Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

#### Clause 4

##### Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a sub-processor

providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

- (j) that it will ensure compliance with Clause 4(a) to (i).

#### Clause 5

##### Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by

the data exporter, where applicable, in agreement with the supervisory authority;

- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

#### **Clause 6**

##### **Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case

the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

#### **Clause 7**

##### **Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### **Clause 8**

##### **Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

#### **Clause 9**

##### **Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

#### **Clause 10**

##### **Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

## Clause 11

### Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## Clause 12

### Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

#### **APPENDIX 1 TO THE EU MODEL CONTRACT**

##### **Data exporter**

Authorized Entities are each a data exporter. The data exporter is a user of services provided by you that in turn rely upon our Services as defined in the MMA.

##### **Data Importer**

The data importer is Alibaba Cloud, a provider a of global cloud computing services.

##### **Data subjects**

Data subjects are described in Attachment 1 to the DPT.

##### **Categories of data**

The personal data transferred are described in Attachment 1 to the DPT.

##### **Processing operations**

The personal data transferred will be subject to the processing activities described in Attachment 1 to the DPT.

#### **APPENDIX 2 TO THE EU MODEL CONTRACT**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational measures implemented are described in Attachment 2 to the DPT.