

MindSphere Data Privacy Terms

October 2018

1. **Purpose, scope and term**

1.1. The Data Privacy Terms (“DPT”) constitute a commissioned 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. If required under Applicable Data Protection Law, you shall enter into data processing agreements with your Authorized Entities that are consistent with the terms of this DPT and comply with the requirements of Applicable Data Protection Law. You shall further 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. Capitalized terms used in this DPT shall have the meaning ascribed to them in Section 13 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) 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**

6.1. You hereby approve the engagement of Subprocessors by us. A current list of Subprocessors commissioned by us is available at www.mindsphere.io/terms.

6.2. We may remove or add new Subprocessors at any time. If required by Applicable Data Protection Law, we will obtain your approval to engage new Subprocessors in accordance with the following process: (i) we shall notify you with at least 20 days’ prior notice before authorizing any new Subprocessor to access your Personal Data either by sending a message to the email address provided to us as part of the ordering process for an Order Form or then associated with your Account or by granting you access to the website referred to in Section 6.1 above that lists all current Subprocessors and provides you with a mechanism to obtain notice of the new Subprocessor; (ii) if you raise no reasonable objections 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 you raise reasonable objections, we will - before authorizing the Subprocessor to access your Personal Data - use reasonable efforts to (a) recommend a change to your 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 your objection; (iv) if the proposed changes or measures cannot eliminate the grounds for non-approval, you may terminate the affected Service with 10 days’ notice following our response to your objection. In the event of termination by you, we will refund any prepaid amounts for the applicable Service on a pro-rata basis for the remainder of the Subscription Term. If you do not terminate the affected Service within the 10 day period, this shall be taken as an approval of the Subprocessor by you.

6.3. 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 6.2 shall apply after your receipt of the notification.

6.4. 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. Transfers to Non-EEA Recipients

7.1. In case Transfers to Non-EEA Recipients relate to Personal Data originating from a Controller located within the EEA or Switzerland, we shall implement the Transfer Safeguards identified per Subprocessor in the list of Subprocessor available at www.mindsphere.io/terms. It is your responsibility to assess whether the respective Transfer Safeguards implemented suffice for you and your Authorized Entities to comply with Applicable Data Protection Law.

7.2. The following shall apply if a Transfer Safeguard is based on the EU Model Contract: Siemens AG enters into such EU Model Contract with the relevant Subprocessor. Each EU Model Contract shall contain the right for you and Authorized Entities to accede to the EU Model Contract. You hereby accede to the EU Model Contracts (as a data exporter) with current Subprocessors and agree that your approval of future Subprocessors in accordance with Section 6.2 shall be deemed as declaration of accession to the EU Model Contract with the relevant future Subprocessor. Furthermore, you agree to procure assent from each of your Authorized Entities (also as data exporters) to accede to such EU Model Contracts. We hereby waive (also on behalf of the respective Subprocessor) the need to be notified of the declaration of accession of you or your Authorized Entities.

7.3. The following shall apply if a Transfer Safeguard is based on the Privacy Shield: We shall contractually bind a Privacy Shield-certified Subprocessor to comply with the Privacy Shield principles with regard to the Personal Data Processed under this DPT.

8. Rectification and erasure

8.1. 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.

8.2. After termination of the MindSphere Agreement, we will delete or anonymize your Personal Data stored on the Platform, 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.

9. 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.

10. Further notifications and support

10.1. 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.

10.2. At your request, we shall reasonably support you in (i) dealing with complaints, requests or orders described in Section 10.1 above (especially in fulfilling your obligation to respond to requests for exercising the 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.

11. Audits

11.1. You shall have the right to audit, by appropriate means - in accordance with Sections 11.2 to 11.5 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.

11.2. 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. 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.

11.3. 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.

11.4. 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.

11.5. 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.

12. Miscellaneous

You shall serve as a single point of contact for us, also with regard to your Authorized Entities and Users under the terms of this DPT. In case this DPT or any other data protection agreement entered into in relation to the Processing of Personal Data (such as EU Model Contracts entered into in accordance with Section 7) provide rights to Controllers (including Controllers other than you) in relation to us and/or our Subprocessors, you shall exercise these rights by contacting us directly, in your own name and/or on behalf of the respective Controller. In case you exercise rights against Subprocessors by contacting us, you hereby authorize us to act on your or the respective Controller's behalf in relation to the Subprocessor. We are entitled to refuse any requests, instructions or claims provided directly by a Controller other than you. We shall be discharged of our obligation to inform or notify a Controller when we have provided such information or notice to you.

13. Definitions

13.1. **"Applicable Data Protection Law"** means all applicable law pertaining to the Processing of Personal Data hereunder.

13.2. **"Authorized Entities"** means (i) your Affiliates, (ii) your OEM Customers as defined in the MindAccess IoT Value Specific Terms or (iii) other legal entities entitled to access and use the Services or employing users entitled to access and use the Services via your designated Account.

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

13.4. **"Country with an Adequacy Decision"** shall mean a country outside the EEA where the European Commission has decided that the country ensures an adequate level of protection with respect to Personal Data.

13.5. **"Data Subject"** means an identified or identifiable natural person.

13.6. **"DPT"** shall mean this Data Privacy Terms.

13.7. **"EEA"** shall mean the European Economic Area.

13.8. **"EU Model Contract"** means 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 or any successor document issued by the European Commission.

13.9. **"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).

13.10. **"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.

13.11. **"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.

13.12. **"Privacy Shield"** means - with regard to Controllers located within the EEA - the European Union / United States Privacy Shield arrangement and - with regard to Controllers located in Switzerland - the Switzerland / United States Privacy Shield arrangement.

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

13.14. **"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.

13.15. **"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.

13.16. **"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.

13.17. **"Transfer Safeguards"** shall mean (i) an adequacy decision in the meaning of Article 45 of the General Data Protection Regulation (EU) 2016/679 or (ii) appropriate safeguards as required by Article 46 of the General Data Protection Regulation (EU) 2016/679.

13.18. **"Transfers to Non-EEA Recipients"** shall mean (i) the Processing of Personal Data outside the EEA or a Country with an Adequacy Decision or (ii) any accesses to Personal Data from outside the EEA or a Country with an Adequacy Decision by us or any of our Subprocessors.

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, the following technical and organizational security measures (TOMs) implemented by us and/or our Subprocessors shall apply.

It is your own responsibility to implement measures in addition to the TOMs described below that fall in your own sphere of responsibility, such as implementing physical and system access control measures for your own premises and assets or configuring the Services to your individual requirements.

1. Physical Access Control

The following measures as implemented are designed to protect against unauthorized physical access to premises, buildings or rooms where data processing systems are located which process and/or use **Personal Data**:

- a) Physical components of the data center facilities, servers, networking equipment, and host software are housed in nondescript facilities.
- b) Physical barrier controls are used to prevent unauthorized entrance to these facilities both at the perimeter (e.g., fencing, walls) and at building access points.
- c) Physical access points to server locations are managed by electronic access control devices and are secured with intrusion detection devices that sound alarms if the door is forced open or held open.
- d) Establishing access authorizations for employees and third parties, including the respective documentation.
- e) All visitors are required to present identification and are signed in.
- f) Use of video cameras (CCTV) to monitor individual physical access to data center facilities.
- g) Data centers utilize security guards 24x7, who are stationed in and around the building.

2. System Access Control

The following measures are implemented to protect against the unauthorized access to and use of data processing systems used to provide Services on the Platform:

- a) User and administrator access to the data center facilities, servers, networking equipment, and host software is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
- b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
- c) IT access privileges are reviewed on a regular basis by appropriate personnel.
- d) Access to systems is revoked within a reasonable timeframe of the employee record being terminated (deactivated).
- e) First time passwords/passphrases are set to a unique value and changed immediately after first use.
- f) User passwords/passphrases are changed periodically and only allow complex passwords.
- g) Time stamped logging of security relevant actions is in place.
- h) Automatic time-out of user terminal if left idle, with user identification and password required to reopen.
- i) Assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.
- j) Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
- k) Firewall policies (configuration files) are pushed to firewall devices on a regular basis.

3. Data Access Control

The following measures are implemented to control that persons entitled to use data processing systems gain access only to the **Personal Data** when they have a right to access, and **Personal Data** is not read, copied, modified or removed without authorization in the course of processing, use and storage.

- a) User and administrator access to the data center facilities, servers, networking equipment, and host software is based on a role based access rights model. A unique ID is assigned to ensure proper user-authentication management for users and administrators on all system components.
- b) The concept of least privilege is employed, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.
- c) IT access privileges are reviewed on a regular basis by appropriate personnel.
- d) Time stamped logging of access to and modification of Personal Data is in place.

- e) An incident response plan is in place to address the following at time of incident:
 - Roles, responsibilities, and communication and contact strategies in the event of a compromise.
 - Specific incident response procedures.
 - Coverage and responses of all critical system components.

4. Data Transmission Control

The following measures are implemented to control that **Personal Data** is not read, copied, modified or removed without authorization during transfer:

- a) Prevention of unauthorized copying by us, our Subprocessors or unauthorized third parties: The measures taken to prevent unauthorized copying of the physical storage infrastructure as such (e.g. copying your data by transferring them to an external storage medium as a hard drive) are included in the measures described above.
- b) Use of role based access rights model: described above.
- c) Firewall policies: described above.
- d) Implement an incident response plan: described above.
- e) Storage Device Decommissioning: When a storage device has reached the end of its useful life, procedures implemented include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices and Applicable Data Protection Law.
- f) Secure access points: there are only a limited number of secure access points to the Platform which allow you to establish a secure communication session with your storage or compute instances within the Services.
- g) Connections to the network by personnel: personnel connect to the network using secure authentication that restricts access to network devices and other cloud components.

5. Data Input Control

The following measures are implemented to retrospectively examine and establish whether and by whom **Personal Data** have been entered, modified or removed from data processing systems used to provide Services on the Platform:

Logging user activity: developers and administrators who need to access to our systems in order to maintain them must explicitly request access. Approved personnel connect to the network using secure authentication that restricts access to network devices and other cloud components, logging all relevant activity for security review. You will enter Personal Data through the usage of the Service and you are hence responsible for implementing and maintaining measures for the establishment of an audit trail to document whether and by whom personal data has been entered into, modified in, or removed from processing.

6. Order Control

The following measures are implemented in order to ensure that Personal Data which are processed on your behalf can only be processed in compliance with your instructions:

- a) Internal communication: various methods of internal communication are implemented at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees and regular management meetings for updates on business performance and other matters.
- b) Corporate segregation: Logically, the production network is segregated from the corporate network by means of a complex set of network security / segregation devices. Developers and administrators on the corporate network who need to access in order to maintain them must explicitly request access. Approved personnel then connect to the network through secure means.
- c) Robust compliance program: The providers of our cloud infrastructure are obliged to (i) implement and maintain a security program that complies, inter alia, with the ISO 27001 or a successor standard (if any) that is substantially equivalent to ISO 27001 and that is designed to provide at least the same level of protection as evidenced by the certification of the providers under ISO 27001 and (ii) have the adequacy of their security measures annually verified by independent auditors.
- d) Policies and security awareness Training: We and our Subprocessors maintain and provide periodic security awareness training to all information system users. Policies and procedures have been established based upon data security and data protection requirements.

7. Availability Control

The following measures are implemented to protect **Personal Data** against accidental or unauthorized destruction or loss:

- a) Fire detection and suppression: Automatic fire detection and suppression equipment has been installed with our data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms.
- b) Redundant power systems: The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.
- c) Climate and temperature control: Personnel and systems monitor and control temperature and humidity at appropriate levels at data centers.
- d) Preventative maintenance: Preventative maintenance is performed to maintain the continued operability of the data center equipment.

8. Data Separation Control

The following measures are implemented to control that Personal Data collected for different purposes can be processed separately:

- a) Multi-tenant environment: The Platform is a virtualized, multi-tenant environment. Security management processes and security controls designed to isolate each customer from other customers are implemented. Systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.
- b) Corporate segregation: described in Section 6 above.