SIEMENS

MindSphere Data Privacy Terms

October 2019

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, Switzerland, or the United Kingdom, 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 Contact. 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 Contact 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 or BCR-P: We shall contractually bind such Subprocessor to comply - as the case may be - with the Privacy Shield principles or BCR-P 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. **Single point of contact and liability**

12.1. 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.

12.2. In case this DPT or any of the Transfer Safeguards in Section 7 (such as EU Model Contract) 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.

12.3. In case the DPT or any of the Transfer Safeguards contain notification obligations vis-a-vis Controllers, we shall be discharged of our obligation to notify a Controller when we have provided such notice to you.

12.4. Without prejudice to the statutory rights of data subjects, limitations of liability contained in the MindSphere Agreement shall also apply to our and our Subprocessors' liability (taken together in the aggregate) vis-à-vis you and your Authorized Entities under the DPT (and any of the Transfer Safeguards specified in Section 7).

12.5. You shall be responsible to ensure that the limitations contained in Sections 12.1 to 12.4 above are enforceable by us and our Subprocessors vis-à-vis your Authorized Entities.

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 Specifc 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. "**Binding Corporate Rules for Processor**" or "**BCR-P**" shall mean Binding Corporate Rules for Processors approved in accordance with Article 47 of the General Data Protection Regulation (EU) 2016/679.

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

13.5. "**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.

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

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

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

13.9. "**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.

13.10. "**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).

13.11. "**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.

13.12. "**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.

13.13. "**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.

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

13.15. "**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.

13.16. "**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.

13.17. "**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.

13.18. "**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.

13.19. **"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.

SIEMENS

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 Personal Data Processed and contained in Content may include: name, phone number, email address, time zone, address data, system access / usage / authorization data, and any system log-files containing Personal Data or any other application-specific data which Users enter into the Service.

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.

SIEMENS

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 and Environmental Security

We implement suitable measures to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers and related hardware). This shall be accomplished by:

a) establishing security areas;
b) protecting and restricting access paths;
c) securing the decentralized data processing equipment and personal computers;
d) establishing access authorizations for employees and third parties, including the respective documentation;
e) regulations on access cards;
f) restrictions on access cards;
g) all access to the data center where Personal Data is hosted will be logged, monitored, and tracked;
h) the data center where Personal Data is hosted is secured by restricted access controls, and other appropriate security measures; and
i) maintenance and inspection of supporting equipment in IT areas and data centers shall only be carried out by authorized personnel.

2. Access Control (IT-Systems and/or IT-Application)

2.1 We implement a roles and responsibilities concept.
2.2 We implement an authorization and authentication framework including, but not limited to, the following elements:
a) role-based access controls implemented;
b) process to create, modify, and delete accounts implemented;
c) access to IT systems and applications is protected by authentication mechanisms;
d) appropriate authentication methods are used based on the characteristics and technical options of the IT system or application;
e) access to IT systems and applications shall require, at least, two-factor authentication for privileged accounts;
f) all access to personal data is logged, monitored, and tracked;
g) authorization and logging measures for inbound network connections to IT systems and applications (including firewalls to allow or deny inbound network connections) implemented;
h) privileged access rights to IT systems, applications, and network services are only granted to individuals who need it to accomplish their tasks (least-privilege principle);
i) privileged access rights to IT systems and applications are documented and kept up to date;
j) access rights to IT systems and applications are reviewed and updated on regular basis;
k) password policy implemented, including requirements re. password complexity, minimum length and expiry after adequate period of time, no re-use of recently used passwords;
l) IT systems and applications technically enforce password policy;
m) access rights of employees and external personnel to IT systems and applications is removed immediately upon termination of employment or contract; and
n) use of secure state-of-the-art authentication certificates.
2.3 IT systems and applications lock down automatically or terminate the session after exceeding a reasonable defined idle time limit.
2.4 We limit privileged access to cloud assets to single or specific ranges of IP addresses.
2.5 Privileged access to cloud assets is done through a bastion host.
2.6 We maintain log-on procedures on IT systems with safeguards against suspicious login activity (e.g. against brute-force and password guessing attacks).

3. Availability Control

3.1 We protect systems and applications against malicious software by implementing appropriate and state-of-the-art anti-malware solutions.
3.2 We define, document and implement a backup concept for IT systems, including the following technical and organizational elements:
a) backups storage media is protected against unauthorized access and environmental threats (e.g., heat, humidity, fire);
b) defined backup intervals; and
c) the restoration of data from backups is tested regularly based on the criticality of the IT system or application.
3.3 We store backups in a physical location different from the location where the productive system is hosted.

3.4 IT systems and applications in non-production environments are logically or physically separated from IT systems and applications in production environments.
3.5 Data centers in which Personal Data are stored or processed are protected against natural disasters, physical attacks or accidents.
3.6 Supporting equipment in IT areas and data centers, such as cables, electricity, telecommunication facilities, water supply, or air conditioning systems are protected from disruptions and unauthorized manipulation.

4. Operations Security

4.1 We maintain and implement an Information Security Framework which is regularly reviewed and updated.
4.2 We log security-relevant events, such as user management activities (e.g., creation, deletion), failed logons, changes on the security configuration of the system on IT systems and applications.
4.3 We continuously analyze the respective IT systems and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities.
4.4 We scan and test IT systems and applications for security vulnerabilities on a regular basis.
4.5 We implement and maintain a change management process for IT systems and applications.
4.6 We maintain a process to update and implement vendor security fixes and updates on the respective IT systems and applications.
4.7 We irretrievably erase data or physically destroys the data storage media before disposing or reusing of an IT system.

5. Transmission Controls

5.1 We document and update network topologies and its security requirements on regular basis.
5.2 We continuously and systematically monitor IT systems, applications and relevant network zones to detect malicious and abnormal network activity by
a) firewalls (e.g., stateful firewalls, application firewalls);
b) proxy servers;
c) Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS);
d) URL Filtering; and
e) Security Information and Event Management (SIEM) systems.
5.3 We administer IT systems and applications by using state-of-the-art encrypted connections.
5.4 We protect the integrity of content during transmission by state-of-the-art network protocols, such as TLS.
5.5 We encrypt, or enable you to encrypt, your data that is transmitted over public networks.
5.6 We use secure Key Management Systems (KMS) to store secret keys in the cloud.

6. Security Incidents

We maintain and implement an incident handling process, including but not limited to
a) records of security breaches;
b) customer notification processes; and
c) an incident response scheme to address the following at time of incident:(i) roles, responsibilities, and communication and contact strategies in the event of a compromise (ii) specific incident response procedures and (iii) coverage and responses of all critical system components.

7. Asset Management, System Acquisition, Development and Maintenance

7.1 We identify and document information security requirements prior to the development and acquisition of new IT systems and applications as well as before making improvements to existing IT systems and applications.
7.2 We establish a formal process to control and perform changes to developed applications.
7.3 We plan and incorporate security tests into the System Development Life Cycle of IT systems and applications.
7.4 We implement an adequate security patching process that includes:
a) monitoring of components for potential weaknesses (CVEs);
b) priority rating of fix;
c) timely implementation of the fix; and
d) download of patches from trustworthy sources.

8. Human Resource Security

8.1 We implement the following measures in the area of human resources security:
a) employees with access to Personal Data are bound by confidentiality obligations; and
b) employees with access to Personal Data are trained regularly regarding the applicable data protection laws and regulations.
8.2 We implement an offboarding process for our employees and external vendors.