Data Processing and Protection Data Sheet

IBM MaaS360 Mobile Device Management (SaaS)

1. Categories of Data Subjects

Data Subjects of any Client Personal Data that generally can be processed in this Cloud Service may include Client's and its affiliates' employees, contractors, business partners, or customers, and to the extent required by law any other legal entities whose personal data is processed by the Cloud Service.

IBM will process Personal Data of all Data Subjects listed above in accordance with the Agreement. Given the nature of the Services, Client acknowledges that IBM is not able to verify or maintain the above list of Categories of Data Subjects. Therefore, if Client will not use this Cloud Service with all the Data Subjects as set out above, then Client is responsible for providing complete, accurate, and up-to-date information to IBM on the actual Data Subjects from within the above list that Client will process in this Cloud Service via Additional Instructions to IBM as set out in the IBM Data Processing Addendum (DPA).

2. Personal Data

The lists as set out below are the Types of Personal Data and Special Categories of Personal Data that generally can be processed within this Cloud Service. IBM will process all Types of Personal Data and Special Categories of Personal Data listed below in accordance with the Agreement. Given the nature of the Services, Client acknowledges that IBM is not able to verify or maintain the below lists of Types of Personal Data and Special Categories of Personal Data. Therefore, if Client will not use this Cloud Service for all the Types of Personal Data and Special Categories of Personal Data as set out below, then Client is responsible for providing complete, accurate, and up-to-date information to IBM on the actual Types of Personal Data and Special Categories of Personal Data from within the below list that Client will process in this Cloud Service via Additional Instructions to IBM as set out in the DPA.

2.1 **Types of Personal Data**

- Basic Personal Information (such as name, address, phone number, email, etc.)
- Technically Identifiable Personal Information (such as device IDs, usage based identifiers, static IP address, etc. - when linked to an individual)
- Personal Location Information (such as geolocation data)

2.2 **Special Categories of Personal Data**

- This Cloud Service was not designed to process any Special Categories of Personal Data.

3. Processing Activities

The processing activities with regard to Client Content (including Client Personal Data) within this Cloud Service include:

- Receipt of Content from Data Subjects and/or third parties
- Computer processing of Content, including data transmission, data retrieval, data access, and network access to allow data transfer if required
- Technical customer support involving Content at Customer request, including monitoring, problem determination, and problem resolution
- Transformation and transition of Content as necessary to deliver the Cloud Service
- Storage and associated deletion of Content
- Backup of Content

4. Duration of Processing

- The duration of Processing within this Cloud Service corresponds to the duration of the Cloud Service. IBM will remove Content (including any Client Personal Data) that is stored or persisted within this Cloud Service at the time of termination or expiration of the Cloud Service.

5. Technical and Organizational Measures

The following Technical and Organization Measures (TOMs) apply to all Content processed by IBM within this Cloud Service (including Client Personal Data):

5.1 **Base Technical and Organizational Measures**

IBM's foundational Technical and Organizational Measures for data protection within its Cloud Services are as described in IBM's Data Security and Privacy Principles for IBM Cloud Services (https://www.ibm.com/cloud/data-security), or as otherwise described below or within the specific Cloud Service Description (https://www.ibm.com/software/sla/sladb.nsf/sla/sd).

5.2 **Amendment to TOMs**

This cloud service makes the following Amendments to the foundational TOMs as described within IBM's Data Security and Privacy Principles for IBM Cloud Services:

- This section is intentionally left blank.

5.3 **Additional TOMs**

The following additional TOMs are applicable to this Cloud Service:

5.3.1 Data Protection

- Client Content is encrypted when transmitted by IBM on any public networks.
- Client Content is encrypted when transmitted by IBM within the Cloud Service's private datacenter network.
- Client Content is encrypted at rest within the IBM Cloud Datacenter.

5.3.2 Business Continuity

- The Cloud Service has Business Continuity plans in place to provide for the recovery of both the Cloud Service, and the associated Client Content, within hours in the event of a corresponding disaster.

5.4 **Certifications**

This Cloud Service provides the following industry recognized compliance, certifications, attestations, or reports as one measure of proof of this Cloud Service's implementation of these Technical and Organizational Measures:

- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- DOD DISA Impact Level 2
- Federal Information Security Management Act (FISMA) Impact Level Moderate
- FedRAMP Moderate Impact Level
- SOC2 Type 2

6. Deletion and Return of Content

- Client can make a copy of their Content (including Client Personal Data) at any time prior to termination or expiration of the Service via the use of self service options available within the Cloud Service.
- Client may also request removal of Content (including Client Personal Data) at any time prior to termination or expiration of the Cloud Service.

7. IBM Hosting and Processing Locations

The following IBM data hosting and processing locations are utilized for this Cloud Service. Client may be able to request that IBM utilize a subset of these locations.

- IBM Data Hosting Locations:
  - France
  - Germany
  - India
  - Netherlands
  - Singapore
  - United States
- IBM Data Processing Locations:
  - Australia
  - France
  - Germany
  - India
  - Ireland
  - Japan
  - Netherlands
  - Singapore
  - United Kingdom
  - United States
- The IBM legal entities associated with each of the IBM Data Hosting and IBM Data Processing Locations set out above are Subprocessors and can be found at https://www.ibm.com/cloud/subprocessors.

8. Third Party Sub-Processors

This Cloud Service involves the following third party Sub-processors in the Processing of Content, including Client Personal Data:

- Akamai (for data processing), United States
- Amazon Web Services, Inc. (for data processing), United States
- Apple Inc. (for data processing), United States
- Google Inc. (for data processing), United States
- Microsoft Corp. (for data processing), United States
- Samsung Electronics Co., Ltd. (for data processing), Korea, Republic of
- Any changes to Sub-processors will be communicated via update of this document as published on https://www.ibm.com/software/sla/sladb.nsf/sla/sd. Additional details on each 3rd party sub-processor are available upon request.

9. International Data Transfer

- EU Standard Contractual Clauses signed by all IBM Data Importers, if applicable, are available at: https://www.ibm.com/software/sla/sladb.nsf/sla/eumc.
- IBM's Privacy Shield Privacy Policy for Cloud Services (https://www.ibm.com/privacy/details/us/en/privacy_shield.html) applies to this Cloud Service for any personal data transferred from the European Economic Area (EEA) to the United States. This Policy does not apply when clients choose to have their offering content hosted in other countries.

10. Privacy Contact and Customer Notifications

- The general privacy contact for IBM Cloud Services is DPA.Help.project@uk.ibm.com.
- A self service portal is also available at mycloudservices.ibm.com to allow subscribed customers to sign up for push notifications of any changes to the data processing or technical and organizational measures associated with this IBM Cloud service.

11. Data Privacy Officer and Other Controllers

- Client is responsible for providing complete, accurate and up-to-date information about its data privacy officer and any other Controllers (including their data privacy officer). Please see the Privacy Contact and Customer communications section for contact information.