Introduction

The following is a summary of the Personal Data that MaaS360 collects and processes and how it is used and shared.

NOTE: This information is provided as-is for information purposes only. It is not a legal representation related to the handling of Client personal data.

For a current set of official Data Privacy Polices and Technical Organization Measures and other related supporting information, please refer to the following:

- IBM Cloud Services Agreement
  - https://www.ibm.com/support/customer/pdf/csa_us.pdf

- IBM Data Processing Addendum and Technical Organizational Measures
  - https://www-05.ibm.com/support/operations/zz/en/dpa.html
  - https://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp

- Cloud Services Service Description (with links to Data Sheets for IBM MaaS360)
  - https://www-03.ibm.com/software/sla/sladb.nsf/sla/sd-6741-21

- Data Processing Addendum, Technical Organizational Measures and Subprocessors for IBM Cloud Technology Support Services
  - https://www.ibm.com/mysupport/s/article/support-privacy

A: Input (How does IBM receive what kind of Personal Data)

1. Categories of Data Subjects

    a. Client's employees
    b. Client's end users
    c. Client's non-employee users (business partners, contractors, etc.).

2. Means of collection of the Personal Data

    a. Client Personal Data is typically collected using the following mechanisms:
        i. Client Administrator provides the information.
            - An example is to create an enrollment request with user corporate email and phone number. Email and SMS may be used to send notifications.
        ii. From the device directly.

- IP Address, location, app inventory and device identifiers may be provided by enrolled devices.

iii. Integration with Client systems (email systems, corporate directories, other Cloud services).

- Functions such as self-service enrollment and group-based policy assignments.

B: IBM Data Processing (What happens with the Data – where is the data going? Who has logical & physical access)

1. Physical storage/hosting of the Personal Data (primary data center, back-up, archives, mirroring, hard copies, removal media).

- The following listed IBM and Third-Party entities provide primary, back-up and offsite data storage.
- IBM Entities (EU/EEA).

Location	Hosting	Other Processing	Platform	Model	Legal Entity
United States	Yes	Yes	IBM Cloud	Private	IBM Corp., USA
Germany	Yes	No	IBM Cloud	Private	IBM Deutschland GmbH
Netherlands	Yes	No	IBM Cloud	Private	IBM Netherlands
France	Yes	No	IBM Cloud	Private	IBM France
Singapore	Yes	No	IBM Cloud	Private	IBM Singapore Pte Ltd
India	Yes	Yes	IBM Cloud	Private	IBM India Pvt Ltd.

- 3rd Parties (EU/EEA)

Vendor	Vendor Function	Access to Client Data **	From Country/Region	Address
Amazon.com Inc.	Application Log and Backup Storage	Yes	United States	440 Terry Avenue North, Seattle, WA 98109, United States

2. Processing operation (what is done with the Personal Data?)

    - MaaS360 is a device management solution where devices and users are provisioned in the system where Personal Data is required to effectively operate the solution.
    - For example, for provisioning, the system requires certain Personal Information, such as the user's phone number (optional), and a corporate email address to send instructions for enrollment.
    - Once the device is enrolled, notifications may be sent (compliance and service related information) from time to time, for which the corporate email or phone number may be used (SMS).
    - The data collected from a user's enrolled devices (IP Address, Location, etc.) are used by Administrators for troubleshooting, inventory and compliance evaluation.
    - The customer administrators can view PI information for audit and inventory purposes.
    - The device and user data input or synched from customer directories can also be used to create groupings - for example groups can be created based on operating system information or user department. In general, groups can be created by any attribute collected by MaaS360.
    - Customer administrator use these groups to send "actions" from the MaaS360 solution. These actions can be manual - initiated by a portal administrator or automated based on rules created using data attributes.
    - Device and user data may also be provided to 3rd parties for critical functions. For example, to notify a user of a request to enroll, an SMS service may be used.
    - Device messaging and application deployment require that certain information be provided to partners like Apple and Google. This typically takes the form of a unique device identifier.
    - MaaS360 Mobile Metrics uses multiple data values to build aggregated metrics. MaaS360 takes steps to reduce the risk that individual data subjects can be reidentified using the following techniques:
        - **Anonymization at a customer level**: For every customer willing to participate in Mobile Metrics, the attributes are aggregated across devices without any reference to a device or a user identifier. As part of the aggregation, device and user identifiers are removed and only aggregated values are retained. If the applicable records (device, apps, etc) for a given customer are less than 5 then this data is not used to build the metric.
        - **Anonymization across customers**: The aggregated values for a customer are further aggregated across all participating customers. Importantly, all the aggregated values within a customer or across customers are then stored without any reference to the customer's

identifiers such as company name, billing ID, location, address. The same applies for any device / user data as well. Any aggregates/trends are kept without reference to device/user's actual identifiers.

- The aggregated data across all customers is used to show reports which provide informational benchmarks. Some examples of reports include:
    a. %Devices by Platform (OS - iOS, Android),
    b. %Devices by Manufacturer
    c. Most Popular Apps (iOS and Android) etc.,
- It is not possible to correlate attributes that are included in different reports. Information in reports is displayed only as Percentage and not as item count.
- A customer can opt out of Mobile Metrics and avoid having their aggregated data is included in reporting.

3. Physical access to the Personal Data (e.g. Hardware maintenance, etc.)

    - Physical Access to the data is limited to Data Center Operations staff only.
    - Physical Access is required to operate the platform, maintain and upgrade systems and perform typical operations activities.
    - IBM Entities (EU/EEA).

Location	Hosting	Other Processing	Platform	Model	Legal Entity
United States	Yes	Yes	IBM Cloud	Private	IBM Corp., USA
Germany	Yes	No	IBM Cloud	Private	IBM Deutschland GmbH
Netherlands	Yes	No	IBM Cloud	Private	IBM Netherlands
France	Yes	No	IBM Cloud	Private	IBM France
Singapore	Yes	No	IBM Cloud	Private	IBM Singapore Pte Ltd
India	Yes	Yes	IBM Cloud	Private	IBM India Pvt Ltd.

    - 3rd Parties (EU/EEA)

Vendor	Vendor Function	Access to Client Data **	From Country/Region	Address
Amazon.com Inc.	Application Log and Backup Storage	Yes	United States	440 Terry Avenue North, Seattle, WA 98109, United States

4. Logical access to the Personal Data (for Service Provision, Support, Maintenance, Super Admin Access, etc.)

    - In addition to individuals that have physical access to personal data, there are individuals that have logical access to perform various activities.
    - These activities include 1st, 2nd, 3rd Level Support, Master Admin, Maintenance, etc.
    - Only IBM Entities are involved in these activities.
    - IBM Entities with Logical Access (EU/EEA)

Location	Hosting	Other Processing	Platform	Model	Legal Entity	Address
United States	Yes	Yes	IBM Cloud	Private	IBM Corp., USA	1 Orchard Road, Armonk, NY 10504

India	Yes	Yes	IBM Cloud	Private	IBM India Pvt Ltd.	Embassy Golf Links, A-Block, 3F, Kormangala Intri Ring Rd., Bangalore-71
Ireland	No	Yes	IBM Cloud	Private	IBM Ireland Ltd	IBM House, Shelbourne Road, Dublin 4. Ireland
Japan	No	Yes	IBM Cloud	Private	IBM Japan Ltd.	Nihonbashi Hazozaki-cho, Chuoku, Tokyo
Israel	No	Yes	IBM Cloud	Private	IBM Israel Ltd.	94 shlomo shmeltzer 49527 Petach-Tikva

5. Limited Personal Data may be shared with 3rd parties to assist in the efficient operation of the platform.
    - Physical Access to the data is limited to Data Center Operations staff only.
    - The following table lists 3rd party entities are involved in these activities and the function they perform.
    - 3rd Parties (EU/EEA)

Vendor	Vendor Function	Access to Client Data	From Country/Region	Address
Amazon Web Services, Inc	Application logs, Instance Backups (encrypted) and SMS Messaging	Yes	United States	1200 12th Ave S, Ste 1200, Seattle, WA 98144, United States
Google Inc.	Device and Application Messaging	Yes	United States	1600 Amphitheatre Parkway, Mountain View, CA 94043United States
Apple Inc.	Device and Application Messaging	Yes	United States	1 Infinite Loop, Cupertino, CA 95014, United States
Microsoft Corp.	Device and Application Messaging	Yes	United States	One Microsoft Way, Redmond, WA 98052, United States
Samsung Electronics Co., Ltd.	Device and Application Messaging	Yes	South Korea	129 Samsung-Ro, Maetan-3dong, Yeongtong-gu, Suwon, 443-742, South Korea

C: Output / Deletion

1. Output/return of Personal Data

    a. Other than backups and the limited Personal Data sharing with 3rd parties, client data is not moved out of the MaaS360 instance or across MaaS360 instances or geographic regions.
    b. Personal Data can be provided/returned to the customer on request. Only the listed IBM Entities are involved in this activity.
    c. IBM Entities.

Location	Legal Entity	Address
United States	IBM Corp., USA	1 Orchard Road, Armonk, NY 10504
India	IBM India Pvt Ltd.	Embassy Golf Links, A-Block, 3F, Kormangala Intri Ring Rd., Bangalore-71

2. Destruction/deletion of Personal Data

    a. Destruction of customer Personal Data is performed within 90 days of the end of a customer contract or upon request.
    b. This is performed by a limited number of Operations individuals that have appropriate access.
    c. It is performed by the listed IBM entities only.
    d. IBM Entities.

Location	Legal Entity	Address
United States	IBM Corp., USA	1 Orchard Road, Armonk, NY 10504
India	IBM India Pvt Ltd.	Embassy Golf Links, A-Block, 3F, Kormangala Intri Ring Rd., Bangalore-71

D: Nice to have included

1. Data Encryption

    a. Data at rest in the MaaS360 instance database is fully encrypted using a AES-256 cryptographic mechanism. This is performed as a normal part of the operation of the platform and is monitored by operations staff. The key is held within the MaaS360 instance and protected by implemented access controls. Encryption Keys for databases are generated by DBAs and turned over to security team for storage.
    b. For Backups, the entire payload is then encrypted again using GPG before being sent offsite.
    c. Only a very limited number of Security Team individuals have access to keys and have the ability to decrypt the data.