

## PERSONAL DATA PROCESSING IN HPE'S OPSRAMP SOLUTION

### 1. WHY DOES OPSRAMP NO LONGER HAVE A DATA PROCESSING AGREEMENT (DPA) ASSOCIATED WITH IT?

The GDPR requires companies to put a data processing agreement in place when they process personal data **on behalf of** their customers. OpsRamp is software-as-a-service offering that provides an IT operations management platform (ITOM) (the “**Service**”). While HPE (including OpsRamp, a Hewlett Packard Enterprise Company) (collectively referred to as HPE) processes certain business contact information of the users in providing the Service, in all instances it does so as a data controller and not as a processor on behalf of the customers. More specifically, HPE determines the purpose and the means of processing (as further described below) and does not act on the instructions of its customers when processing such business contact information.

Therefore, HPE is deemed a data controller under the GDPR.

### 2. WHAT PERSONAL DATA IS USED IN OPSRAMP SERVICES?

HPE processes the business contact information of OpsRamp users, more specifically the following information: first name, last name, email address and phone number (“**Personal Data**”).

### 3. HOW IS THE PERSONAL DATA USED IN OPSRAMP SERVICES?

The Personal Data is used during the delivery of the Service in the following ways:

#### **A) Granting access to OpsRamp application**

- (i) creating first user (admin) accounts in the platform
- (ii) viewing the Personal Data of the admins and end users (who are set up as authorized users by customer admins)
- (iii) sending email communications to the customers (through Mailgun and SendGrid applications)

#### **B) Collection of audit logs by OpsRamp application**

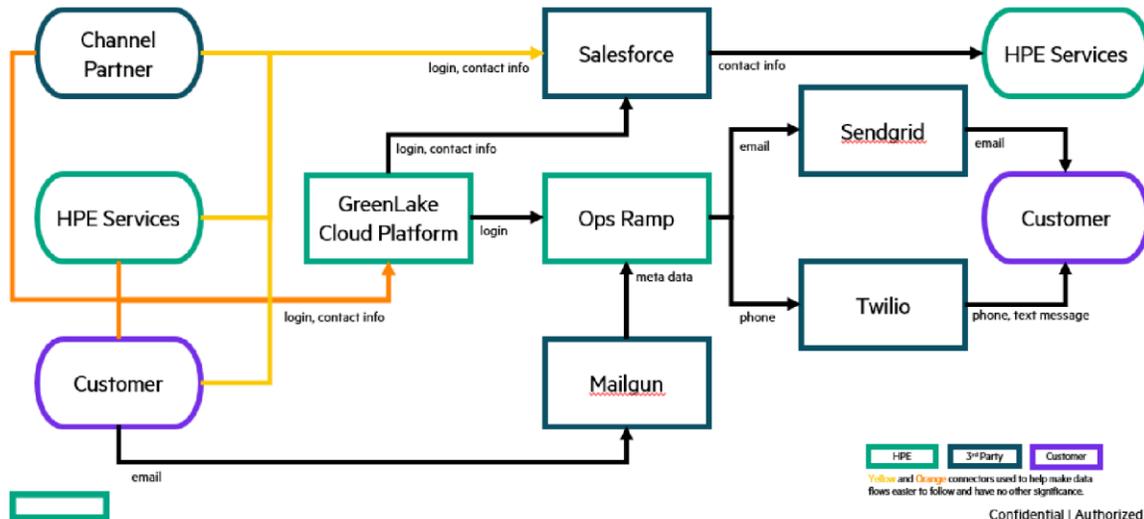
The application collects audit logs that store information on users logging into the OpsRamp application once access is provided. These logs include, user login, logout, password, access issues, activity performed on the Opsramp application, such as creating and deleting users, resources and permissions on the platform, login, logout errors etc. These reports are available to customer admin and HPE admin for viewing.

#### **C) Provision of support services**

HPE uses Personal Data to send updates about support tickets and contact users for troubleshooting purposes. **D) Contract management**

Personal Data is used by HPE for contract management purposes, including tracking customer’s performance via regular operational reviews as well as billing.

### OpsRamp data flow



Confidential | Authorized | 1

Please also see below a detailed data map for OpsRamp.

#### 4. CAN HPE POTENTIALLY ACCESS ANY OTHER PERSONAL DATA?

OpsRamp application has *logs and traces* functionality. The logs collected from application (as configured by customers) may carry personal information (other than Personal Data depending on the customer's configuration) which is stored in plain text on OpsRamp platform (for 30 days). OpsRamp platform does not have the capability to identify and encrypt the personal information at the data source. The customer has the sole capability and responsibility to restrict sending personal information to the platform.

Since the Service does not include the processing of personal data on behalf of customer, HPE encourages all customers to use privacy by design best practices to limit disclosure of personal data to only those individuals and third parties with a need to know such information.

#### 5. HOW DOES HPE PROTECT CUSTOMER PERSONAL DATA WHEN ACTING AS A DATA CONTROLLER?

When acting as a data controller, HPE processes Personal Data in compliance with applicable laws and its Privacy Statement (<https://www.hpe.com/us/en/legal/privacy.html>).