HPE Device Entitlement Gateway (DEG) as a Service

Annex II: Description of the processing

1.	Description of processing	As part of providing software maintenance support and professional services, Processor may have access to data stored in the Processor Device Entitlement Gateway (DEG) platform (including metadata). This data may include Controller personal data.
2.	Type of personal data processed	The type of personal data processed will depend on the data the Controller has stored on the business applications (including metadata), IT, and network infrastructure and it includes following personal data: IMSI, MSISDN, Device ID (IMEI, EID, ICCID), IP Address, Cookie.
3.	Categories of personal data processed	Any data subject whose personal data is stored by the Controller on the business applications (including metadata), IT, and network infrastructure including device identification data, electronic communications metadata, authentication data.
4.	Duration of processing	Processor shall process Controller personal data for the duration of the Agreement and/or any applicable transaction document. All the personal data will be stored in the DEG platform for maximum of 6 months.
5.	Technical & Organizational Measures	Processor shall maintain the information and physical security program for the protection of Controller personal data as detailed in Annex III below.

HPE Device Entitlement Gateway (DEG) as a Service

Annex III: Technical and organizational measures including technical and organizational measures to ensure the security of the data

1. As part of the Processor information and physical security program for the protection of Controller personal data ("Security Program"),HPE conducts periodic reviews of security practices against industry standards, such as NIST, ISO 27001, and SOC. Processor regularlyre-evaluates and updates the Processor Security Program as the industry evolves, new technologies emerge, or new threats are identified.

2. The Processor Security Program consists at least of the following:

   a. Processor maintains physical security standards designed to prohibit unauthorized physical access to Processor facilities andequipment by using the following practices:

      i. Physical access to locations is limited to Processor employees, subcontractors, and authorized visitors

      ii. Processor employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on-premises

      iii. Monitoring access to Processor facilities, including restricted areas and equipment within facilities

iv. Access to the data center where Controller personal data is hosted is logged, monitored, and tracked; and

v. Data centers are secured with alarm systems and video cameras.

b. Processor maintains access control of the relevant IT environment in accordance with industry best practices. These controls includebut are not limited to requirements regarding principles of least privilege and password complexity and use.

c. Processor infrastructure has reasonable up-to-date versions of system security software which may include host firewall, anti-virusprotection, and up-to-date patches and virus definitions. Processor maintains logs of events involving the infrastructure, includingintrusion detection systems to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and othersecurity risks.

3. Upon request, Processor will review with Controller a summary of vulnerability assessments. Vulnerability assessments shall not entitleController to view, or in any way access records and/or processes: (a) not directly related to the service; (b) in violation of applicable laws;and/or (c) in violation of Processor's confidentiality and security obligations owed to a third party.

4. Employees and contractors are trained on Processor's privacy and security policies and made aware of their responsibilities with regardto privacy and security practices. Processor employees and contractors are contractually bound to maintain the confidence of Controllerpersonal data and comply with applicable Processor policies, standards, or requirements in relation to the processing of Controllerpersonal data. Failure to comply with those policies, standards, or requirements will be subject to investigation which may result indisciplinary action up to and including termination of employment or engagement by Processor.

5. In the event Processor confirms a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorizeddisclosure of, or access to, Controller personal data ("Security Incident"), Processor will:

   a. Without undue delay, notify Controller of the Security Incident. Processor will provide Controller with updates on the status of theSecurity Incident until the matter has been remediated. The reports will include, without limitation, a description of the SecurityIncident, actions taken, and remediation plans. If Controller becomes aware of a Security Incident that affects the services, Controllershall promptly notify Processor of such and inform Processor of the scope of the Security Incident.

   b. At the request and cost of the Controller, (i) provide reasonable assistance to the Controller in notifying a security breach to thesupervisory authority competent under the privacy laws applicable to the Controller; and (ii) provide reasonable assistance to theController in communicating a data breach to data subjects in cases where the data breach is likely to result in a high risk to the rightsand freedoms of individuals.

a50000032ENW - Annex a50009392ENW

HEWLETT PACKARD ENTERPRISE

hpe.com