Hewlett Packard Enterprise

HPE DATA PRIVACY AND SECURITY AGREEMENT SCHEDULE

HPE Device Entitlement Gateway (DEG) as a Service ("Service")

This Data Privacy and Security Agreement ("DPSA") Schedule governs the privacy and security of Personal Data by HPE in connection with the Service on Customer's behalf and is made a part of the agreement between HPE and Customer, or if no agreement exists, HPE's standard terms and conditions ("Agreement").

1. **This DPSA forms part of the Agreement.** To the extent there are any conflicts between the terms of this DPSA and the Agreement, the DPSA shall prevail.

2. **Definitions**

2.1. "Personal Data" or "Customer Personal Data" means any (Customer) information relating to an identified or identifiable natural persons or as otherwise defined in applicable Privacy Laws.

2.2. "Business Contact Data" means contact information of Customer's representatives for (i) invoicing, billing, and other business inquiries, (ii) information on Customer's usage of the Service, and (iii) other information that HPE collects and needs to communicate with Customer.

2.3. "Privacy Laws" mean all applicable laws and regulations relating to the Processing of Personal Data and privacy that may exist in the relevant jurisdictions.

2.4. "Controller" means the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data in accordance with applicable Privacy Law.

2.5. "Processor" means any natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Controller or on the instruction of another Processor acting on behalf of a Controller.

2.6. "Process," "Processing," or "Processed" means an operation or set of operations performed on or with Personal Data whether or not by automatic means (including, without limitation, accessing, collecting, recording, organizing, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing, and destroying Personal Data) and any equivalent definitions in Privacy Law to the extent that such definition should modify this definition.

2.7. "Special Category Data" means Customer Personal Data which relates to an individual's racial/ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, biometric data (if used for the purpose of uniquely identifying an individual) or genetic data.

3. **Appointment and Instructions**

3.1. HPE shall Process Customer Personal Data as necessary to provide the Service and to meet HPE's obligations under this DPSA, the Agreement, and applicable Privacy Law as a service provider and Processor of Customer Personal Data. Details of the Processing including the subject matter, purpose and duration of the Processing the types of personal data and categories of data to whom the data are set out in Exhibit A.

3.2. HPE shall Process Customer Personal Data in accordance with Customer's instructions as set out in this DPSA, the Agreement, or other documented instructions between HPE and Customer. Potential costs and charges associated with such additional instructions shall be agreed pursuant to the terms of the Agreement.

3.3. HPE may Process Customer Personal Data other than on the instructions of Customer if it is required under law applicable to HPE. In this situation, HPE shall inform Customer of such a requirement before HPE Processes Customer Personal Data unless the law prohibits this on important grounds of public interest. If HPE is unable to comply with Customer's instructions or this DPSA due to changes in legislation or, if HPE believes (without having to conduct a comprehensive legal analysis) that any instruction from Customer will violate applicable law or for any other reason, HPE shall promptly notify Customer in writing.

3.4. HPE acknowledges that HPE has no right, title, or interest in Customer Personal Data (including all intellectual property or proprietary information contained therein). HPE may not sell, rent, or lease Customer Personal Data to anyone.

3.5. If Customer uses the Service to Process any categories of data not expressly covered by this DPSA, Customer acts at its own risk and HPE shall not be responsible for any potential compliance deficits related to such use.

4. **Compliance with laws**

4.1. The Parties shall at all times comply with their respective obligations under this DPSA and Privacy Laws that apply to their respective processing of Personal Data. In addition, if HPE interacts with Protected Health Information as defined under the Health Insurance Portability and Accountability Act, the parties agree to comply with the terms of the Business Associate Agreement found at hpe.com/info/customer-privacy.html.

4.2. HPE shall also comply with all applicable laws and HPE's privacy policy with respect to the Processing of Business Contact Data and use Business Contact Data only for legitimate business purposes, including, without limitation, invoicing, collections, service usage monitoring and optimization, service improvements, maintenance, support, professional services, communications relating to contract renewals (directly or through a subprocessor acting on HPE's behalf or an HPE approved reseller for contract renewal purposes), and information about new and additional services.

4.3. Where HPE discloses its personnel's personal data to Customer or HPE personnel provide their personal data directly to Customer, which Customer Processes to manage its use of the Service, Customer shall Process that data in accordance with its privacy policies and applicable Privacy Laws. Such disclosures shall be made by HPE only where lawful for the purposes of contract management, service management, or Customer's reasonable and lawful background screening verification or security purposes.

5. **Security**

5.1. HPE shall implement and maintain the physical, technical, and organizational security measures set out in Exhibit A, as may be supplemented or modified in the applicable transaction document, to protect Customer Personal Data and Business Contact Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure, or access.

5.2. Customer acknowledges that HPE may change the security measures through the adoption of new or enhanced security technologies and authorises HPE to make such changes provided that they do not diminish the level of protection. HPE shall make information about the most up to date security measures applicable to the Service available to Customer upon request.

6. **Subprocessing and Location of Processing**

6.1. Customer authorises HPE to engage affiliated and unaffiliated subprocessors ("Subprocessors") to perform some or all of its obligations under the Agreement. Only where necessary to provide the Service, HPE will provide its Subprocessors with access to Customer Personal Data.

6.2. The Subprocessors applicable to the Service and location of processing can be found at hpe.com/info/customer-privacy.html and are deemed as approved by Customer. Customer will subscribe to HPE's notification tool on the above website, and in the event of changes to approved Subprocessors, HPE will notify Customer via the notice subscription tool. Customer may object to the appointment or replacement of a Subprocessor at any time, and the parties shall use all reasonable endeavours to resolve Customer's objection. If the parties fail to resolve Customer's objection within a reasonable period of time, the matter shall be addressed pursuant to the dispute resolution procedure in the Agreement. In case HPE and customer fail to agree on an amicable resolution to the proposed subprocessor change, HPE shall have a right to terminate the contract without further obligations.

6.3. HPE shall conduct appropriate due diligence of its Subprocessors and execute valid, enforceable, and written contracts with Subprocessors requiring the Subprocessor to abide by terms no less protective than those in this DPSA regarding the Processing and protection of Customer Personal Data (including the EU Model Contract terms relating to data importers in the case of an onward transfer of EU, EEA, or Swiss Personal Data to a non-adequate country).

6.4. HPE remains responsible for the acts and omissions of the Subprocessors it engages to provide the Service to Customers giving rise to a breach of this DPSA as if they were its own acts or omissions.

7. **Audit and Assurance**

7.1. HPE shall arrange for audits of HPE's data Processing and protection practices to confirm compliance with applicable Privacy Law by reputable third-party auditors and provide Customer with a report summary and additional information on request.

7.2. Customer shall have the right to conduct additional audits of HPE's compliance with its obligations under this DPSA in accordance with the Agreement. The audit rights are generally exercised in consultation with HPE. HPE is obliged to assist Customer in such audits and any audits of the competent authorities. These audits must be carried out in consideration of the business processes and HPE's need for security and confidentiality.

7.3. Certain information about HPE's security standards and practices are sensitive confidential information which will not be disclosed by HPE to Customer. Upon request, HPE agrees to respond, no more than once per year, to a reasonable information security questionnaire concerning security practices specific to the Service provided hereunder.

7.4. On Customer's request, HPE shall within a reasonable timeframe make appropriate information available to Customer to demonstrate its compliance with applicable Privacy Law, save where that information is readily available to Customer direct through its use of the Service.

8. **Providing Customer Assistance**

8.1. At Customer's request HPE shall cooperate with Customer and provide Customer with assistance necessary to facilitate the Processing of Customer Personal Data in compliance with Privacy Laws applicable to Customer in relation to HPE Service, including by way of example:

8.1.1. assist Customer by implementing appropriate and reasonable technical and organizational measures, insofar as this is possible, to assist with Customer's obligation to respond to requests from individuals seeking to exercise their rights under the Privacy Laws applicable to Customer;

8.1.2. provide reasonable assistance to Customer in Customer's assessment and implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the Processing and the nature of Customer Personal Data;

8.1.3. the notification of Security Incidents pursuant to Exhibit A;

8.1.4. provide reasonable assistance to Customer in carrying out a privacy impact assessment.

8.2. If Customer requests cooperation or assistance pursuant to this Section, Customer shall notify HPE in writing of the requirements and formulate Customer's instructions. HPE shall respond within a reasonable period of time and provide Customer with approximate time and fee estimates for the implementation of any changes necessary to accommodate Customer's compliance needs. To the extent that compliance with this Section constitutes a change to the scope of the Service, the parties shall, acting reasonably, agree on appropriate change order.

9. **Data Quality, Retrieval and Destruction, Repair, or Replacement Service**

9.1. To the extent that Customer is not able to access Customer Personal Data itself, HPE shall on Customer's written request (i) update, correct, or delete Customer Personal Data; and/or (ii) provide copies of Customer Personal Data.

9.2. Upon termination of the Agreement, HPE shall at the election of Customer return or delete Customer Personal Data and HPE shall not retain copies of Customer Personal Data unless otherwise agreed with Customer or where it is required to do so under applicable law, in which case HPE shall stop actively Processing the data and maintain the security and confidentiality of the data.

9.3. With regard to the repair or replacement of data carriers (server, hard-disks, SSD, flash-disks, memory, etc.), Customer will either purchase the optional (C)DMR Service or adequately wipe (following the NIST Standard) carriers prior to providing them to HPE.

10. **Data Transfers**

10.1. To address the transfer of EU, EEA, UK or Swiss Personal Data by Customer or a Customer affiliate to HPE or an HPE affiliate located in a country which is not approved by the European Commission as providing adequate protection for personal data pursuant to Article 45(3) of the General Data Protection Regulation, the Customer shall rely on HPE's Binding Corporate Rules – Processors (BCR-P). The list of Service subject to HPE BCR-P are listed on BCR website at hpe.com/uk/en/privacy/binding-corporate-rules.html and/or can be provided upon request.

10.2. HPE (and any other HPE company and Subprocessor whom the Customer authorizes to Process Personal Data pursuant to Clause 6 of the DPSA) may receive and/or transfer Personal Data to any country in accordance with the BCR-P. Customer shall ensure that if the transfer involves Special Category Data, that data subjects have been informed of the transfer, or will be informed before the transfer, that this Special Category Data could be transmitted to another country. The BCR-P shall be binding on the Customer by means of the third-party rights set out in Clause 4.1 of the BCR-P which shall include the right to enforce the BCR-P against HPE, including judicial remedies and the right to receive compensation. The BCR-P includes the intercompany agreement and the applicable policies and procedures which form HPE's Binding Corporate Rules for Processors as they apply to the Customer and as developed, amended or updated by HPE from time to time in accordance with the applicable Working Documents adopted by the Article 29 Working Party (and subsequently the European Data Protection Board). A copy of the documentation comprising the BCR-P, which is incorporated by reference and is an integral part of this DPSA, is available to Customer upon written request. Customer shall inform data subjects regarding the existence of Processors outside of the EU/EEA/Switzerland and of Customer's reliance on the BCR-P as required by Privacy Laws and shall make available to data subjects upon request a link to HPE's BCR Rights Notice at hpe.com/uk/en/privacy/binding-corporate-rules.html.

EXHIBIT A – DEVICE ENTITLEMENT GATEWAY (DEG) AS A SERVICE DATA PROCESSING

In this Exhibit, HPE describes the terms specific to Device Entitlement Gateway (DEG) as a service, hereinafter referred to as "Service(s)" for the purpose of this Exhibit E, including its commitment to technical and organizational security measures to protect Customer Personal Data.

HPE performs the following Personal Data Processing as part of the Service	As part of providing software maintenance support and professional services, HPE may have access to data stored in the HPE DEG Platform (including metadata). This data may include Customer Personal Data.
Type of Customer Personal Data Processed	The type of personal data processed will depend on the data the Customer 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
Categories of Data Subjects	Any data subject whose Personal Data is stored by the Customer on the business applications (including metadata), IT and network infrastructure including Device Identification Data, Electronic Communications Metadata, Authentication Data.
Duration of Processing	HPE shall process Customer Personal Data for the duration of the applicable transaction document. All the personal data will be stored in the DEG platform for max 6 months.
Security Measures	HPE shall maintain the following information and physical security program for the protection of Customer Personal Data (the "HPE Security Program").

1. As part of the HPE Security Program, HPE conducts periodic reviews of security practices against industry standards, such as NIST, ISO 27001, and SOC. HPE regularly re-evaluates and updates the HPE Security Program as the industry evolves, new technologies emerge, or new threats are identified.
2. The HPE Security Program consists at least of the following:
   - 2.1. HPE maintains physical security standards designed to prohibit unauthorized physical access to HPE facilities and equipment by using the following practices:
     - 2.1.1 physical access to locations is limited to HPE employees, subcontractors, and authorized visitors;
     - 2.1.2 HPE employees, subcontractors, and authorized visitors are issued identification cards that must be worn while on-premises;
     - 2.1.3 monitoring access to HPE facilities, including restricted areas and equipment within facilities;
     - 2.1.4 access to the data center where Customer Personal Data is hosted is logged, monitored, and tracked; and
     - 2.1.5 data centers are secured with alarm systems and video cameras.
   - 2.2. HPE maintains access control of the relevant IT environment in accordance with industry best practices. These controls include but are not limited to requirements regarding principles of least privilege and password complexity and use.
   - 2.3. Computers and servers have reasonable up-to-date versions of system security software which may include host firewall, anti-virus protection, and up-to-date patches and virus definitions. Software is configured to scan for and promptly remove or fix identified findings. HPE maintains logs of various components of the infrastructure and an intrusion detection system to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other actual and threatened security risks.

3. Upon request, HPE will review with Customer a summary of vulnerability assessments. Vulnerability assessments shall not entitle Customer 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 HPE's confidentiality and security obligations owed to a third party.
4. Employees and contractors are trained on HPE's privacy and security policies and made aware of their responsibilities with regard to privacy and security practices. HPE employees and contractors are contractually bound to maintain the confidence of Customer Personal Data and comply with applicable HPE policies, standards, or requirements in relation to the Processing of Customer Personal Data. Failure to comply with those policies, standards, or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by HPE.
5. In the event HPE confirms a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Personal Data ("Security Incident"), HPE will:
    5.1. without undue delay, notify Customer of the Security Incident. HPE will provide Customer with updates on the status of the Security Incident until the matter has been remediated. The reports will include, without limitation, a description of the Security Incident, actions taken, and remediation plans. If Customer becomes aware of a Security Incident that affects the Service, Customer shall promptly notify HPE of such and inform HPE of the scope of the Security Incident.
    5.2. at the request and cost of the Customer, (i) provide reasonable assistance to the Customer in notifying a security breach to the supervisory authority competent under the Privacy Laws applicable to the Customer; and (ii) provide reasonable assistance to the Customer in communicating a data breach to data subjects in cases where the data breach is likely to result in a high risk to the rights and freedoms of individuals.

Hewlett Packard Enterprise

a50000032ENW, Rev. 2