Hewlett Packard Enterprise

Legal data sheet

Check if the document is available in the language of your choice.

HPE FINANCIAL SERVICES DATA PROCESSING AND SECURITY AGREEMENT SCHEDULE

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

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

1.	Servicer performs the following Services:	Servicer or Servicer's affiliates will provide a data sanitization process with respect to certain equipment ("**Equipment**") tendered to or made available to Servicer or Servicer's affiliates pursuant to the Commercial Agreement (as more particularly described in the Commercial Agreement)
2.	Equipment Data	Any data attached to the Equipment which may include Personal Data that Customer will provide to Servicer for Processing
3.	Personal Data	Means any information relating to identified or identifiable natural persons or as otherwise defined in applicable Privacy Laws
4.	Data Sanitization Process	Means a process by which Servicer will sanitize storage media contained in the Equipment using (i) industry standard software incorporating a three pass overwrite process or (ii) a software/firmware data-area secure erase function on any Equipment where this is a standard functionality built into the Equipment or the storage media contained in the Equipment
5.	Data subjects to whom Customer Data pertains are	Employees or other representatives of Customer
6.	Data subjects to whom Equipment Data pertains are	Employees and clients of Customer
7.	With respect to Customer Data, Customer is acting as	Data Controller
8.	With respect to Equipment Data, Servicer is acting as	Data Processor
9.	Servicer shall process Equipment Data only as follows	Pursuant to the Data Sanitization Process
10.	Customer Data means	Contact information of Customer's employees and other representatives for invoicing, billing and other business inquiries, information on Customer's usage of Services, and other information that Servicer collects and needs to do business with Customer and which may include Personal Data
11.	Privacy Laws	Means all applicable laws and regulations relating to the Processing of Personal Data and privacy that may exist in the relevant jurisdictions, including the GDPR
12.	General Data Protection Regulation or GDPR	Means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (and its implementing legislation), with effect from the 25th of May 2018
13.	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; where the purposes and means of Processing are determined by applicable Privacy Law, the Controller or criteria for the Controller's nomination will be as designated by applicable Privacy Law
14.	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
15.	Process, Processing or Processed	Means an operation or set of operations which 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 exceed this definition
16.	Customer contact for data privacy or security related questions:	Customer contact provided in the Commercial Agreement
17.	Servicer contact for data privacy or security related questions:	Mark Rashid and/or Louise Del Tufo, HPEFS Business Controls & Compliance Colman McCabe, HPEFS Legal Email: colman.mccabe@hpe.com

This DPSA incorporates by reference:

Exhibit A—Data Protection—Base Terms

Exhibit B—Security

Exhibit A—Data Protection—Base Terms

Servicer shall Process Equipment Data subject to the terms of the DPSA. All capitalized terms shall have the meaning defined in the DPSA.

1. Appointment and Instructions

1.1. Servicer shall Process Equipment Data as necessary to provide the Services and to meet Servicer's obligations under this DPSA, the Commercial Agreement and applicable Privacy Law as a service provider and Processor of Equipment Data. The type of Equipment Data Processed includes that set out in the definitions. Servicer shall Process Equipment Data for the duration of the Commercial Agreement or as otherwise agreed by the parties in writing.

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

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

1.4. Servicer acknowledges that Servicer has no right, title or interest in any Equipment Data (including all intellectual property or proprietary information contained therein). Servicer shall not sell, rent or lease Equipment Data to anyone.

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

2. Compliance with Laws

2.1. 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.

2.2. Servicer shall also comply with all applicable laws and Servicer's privacy policy with respect to the Processing of Customer Data and use Customer Data only for legitimate business purposes, including, without limitation, invoicing, collections, service usage monitoring and optimization, service improvements, maintenance, support, communications relating to contract renewals, and information about new and additional services.

2.3. Where Servicer discloses Servicer employee Personal Data to the Customer or a Servicer employee provides Personal Data directly to Customer, which the Customer Processes to manage its use of the Services, Customer shall Process that data in accordance with its privacy policies and applicable Privacy Laws. Such disclosures shall be made by Servicer only where lawful for the purposes of contract management, service management or the Customer's reasonable and lawful background screening verification or security purposes.

3. Security

3.1. Servicer shall implement and maintain the physical, technical and organizational security measures set out in Exhibit B—Security to protect Equipment Data and Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

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

4. Subprocessing & Location of Processing

4.1. Customer authorizes Servicer to engage affiliated and unaffiliated subprocessors ("**Subprocessors**") to perform some or all of its obligations under the Commercial Agreement. Only where necessary to provide the Services, Servicer will provide its Subprocessors with access to Equipment Data.

4.2. The Subprocessors, if any, applicable to the Services 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 the notification tool on the above website, and in the event of changes to approved Subprocessors, Servicer 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 endeavors 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 Commercial Agreement. In case Servicer and Customer fail to agree on an amicable resolution to the proposed Subprocessor change, Servicer shall have a right to terminate the Commercial Agreement without further obligations.

4.3. Servicer 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 Equipment Data.

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

5. Audit and Assurance

5.1. Servicer shall arrange for audits of Servicer'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.

5.2. Customer shall have the right to conduct additional audits of Servicer's compliance with its obligations under this DPSA in accordance with the Commercial Agreement. The audit rights are generally exercised in consultation with Servicer. Servicer 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 Servicer's need for security and confidentiality.

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

5.4. On Customer's request, Servicer 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 Services.

6. Providing Customer Assistance

6.1. At Customer's request, Servicer shall co-operate with Customer and provide Customer with assistance necessary to facilitate the Processing of Equipment Data in compliance with Privacy Laws applicable to Customer in relation to the Services including by way of example:

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

6.1.2. 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 the Equipment Data;

6.1.3. The notification of Security Incidents pursuant to Section 1.4 of Exhibit B—Security;

6.1.4. Provide reasonable assistance to Customer in carrying out a privacy impact assessment.

6.2. If Customer requests co-operation or assistance pursuant to this Section 6, Customer shall notify Servicer in writing of the requirements and formulate Customer's instructions. Servicer 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 6 constitutes a change to the scope of the Services, the parties shall, acting reasonably, agree on appropriate amendments to the Commercial Agreement.

7. Data Quality, Retrieval & Destruction

7.1. Taking into account the nature of the Processing, to the extent that Customer is not able to access Customer Personal Data itself, Servicer shall, on Customer's written request, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising data subject's rights.

7.2. Upon termination of the Commercial Agreement, Servicer shall at the election of Customer return or delete Customer Personal Data and Servicer 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 Servicer shall stop actively Processing the data and maintain the security and confidentiality of the data.

8. Data Transfers

8.1. Except with respect to transfers of data to Servicer's processing facility in the UK, there are no international data transfers as part of the Services.

8.2. To address the transfer of EU, EEA, UK or Swiss Personal Data to Servicer or a Servicer affiliate located in a country which is not approved by the European Commission as providing adequate protection for personal data pursuant to Article 25(6) of the Directive 95/46/EC or Article 45(3) of the General Data Protection Regulation, the Customer may rely on HPE's Binding Corporate Rules—Processors (BCR-P). The list of Services 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.

Exhibit B—Security

1. Security Practices & Review

1.1. Servicer shall maintain the following information and physical security program for the protection of Equipment Data.

1.2. 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. Servicer 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.

1.3. Employees and contractors are trained on Servicer's privacy and security policies and made aware of their responsibilities with regard to privacy and security practices. Servicer's employees and contractors are contractually bound to maintain the confidence of Personal Data and comply with applicable policies of Servicer, standards or requirements in relation to the Processing of Equipment 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 Servicer.

1.4. In the event that Servicer confirms a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to, Equipment Data ("**Security Incident**"), Servicer will:

1.4.1. Without undue delay notify Customer of the Security Incident. Servicer 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 Services, Customer shall promptly notify Servicer of such and inform Servicer of the scope of the Security Incident.

1.4.2. 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.

a50002998ENW, November 2020

Hewlett Packard Enterprise