

HPE Financial Services

Annex II: Description of the processing

<p>1. Description of processing</p>	<p>Processor will perform a Data Sanitization Process with respect to certain equipment (“Equipment”) tendered to or made available to Processor or Processor’s affiliates pursuant to the Agreement (as more particularly described in the Agreement); and/or applicable transaction document, wherein, the term “Data Sanitization Process” means a process by which Processor will sanitize storage media contained in the Equipment in accordance with the measures as set forth in the Agreement. Any data stored on the Equipment, including Controller personal data, will only be processed in accordance with the Data Sanitization Process.</p>
<p>2. Type of personal data processed</p>	<p>The type of personal data processed will depend on the data the Controller has stored on the Equipment and may include sensitive personal data.</p>
<p>3. Categories of personal data processed</p>	<p>Any data subject whose personal data is stored by the Controller on the Equipment including, without limitation, Controller’s clients, end users, employees, contractors, and temporary workers.</p>
<p>4. Duration of processing</p>	<p>Processor shall process Controller personal data for the duration of the Agreement and/or any applicable transaction document.</p>
<p>5. Technical & Organizational Measures</p>	<p>Processor shall maintain the information and physical security program for the protection of Controller personal data as detailed in Annex III below.</p>

HPE Financial Services

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

1. There will be no international data transfers as part of Processor’s service to Controller under this Agreement, except with respect to transfers of data to Processor’s processing facility in the UK.
2. Processor infrastructure has 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. Processor maintains logs of events involving the infrastructure, including intrusion detection systems to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other security risks.

3. Employees and contractors are trained on Processor’s privacy and security policies and made aware of their responsibilities with regard to privacy and security practices. Processor’s employees and contractors are contractually bound to maintain the confidence of personal data and comply with applicable policies of Processor, standards or requirements in relation to the processing of Controller 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 Processor.
4. In the event that Processor confirms a security breach leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Controller personal data (“Security Incident”), Processor will:
 - 4.1 Without undue delay notify Controller of the Security Incident. Processor will provide Controller 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 Controller becomes aware of a Security Incident that affects the services, Controller shall promptly notify Processor of such and inform Processor of the scope of the Security Incident.
 - 4.2 At the request and cost of the Controller: (i) provide reasonable assistance to the Controller in notifying a security breach to the supervisory authority competent under the privacy laws applicable to the Controller; and (ii) provide reasonable assistance to the Controller 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.

Visit [HPE.com](https://www.hpe.com)

[Chat now](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a50002998ENW - Annex a50009452ENW

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

