

HPE Cloud Volume Services

Annex II: Description of the processing

1.	Description of processing	As part of providing Controller access and use of Processor’s cloud based storage and management services, Processor may have access to data stored within Controller’s business applications through Controller’s use of the HPE Cloud Volume Services. 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 through their use of the HPE Cloud Volume Services and may include sensitive personal data.
3.	Categories of personal data processed	Any data subject whose personal data is stored by the Controller through use of the HPE Cloud Volume Services including, without limitation, Controller’s clients, end users, employees, contractors, and temporary workers.
4.	Duration of processing	Processor shall process Controller personal data for the duration of the Agreement and any applicable transaction document.
5.	Technical & Organizational Measures	Processor shall maintain the information and physical security program for the protection of Controllerpersonal data as detailed in Anex III below.

HPE Cloud Volume Services

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

1. Processor implements reasonable measures designed to help secure Controller personal data against accidental or unlawful loss, access, or disclosure. Processor, Processor affiliates, and third-party service providers will only use Controller personal data to maintain or provide the HPE Cloud Volume Services.
2. Controller may specify the Processor regions in which Controller personal data will be stored. Controller consents to the transfer to and storage of Controller personal data in the Processor regions Controller selects. Processor, Processor affiliates, and third-party service providers will not access or use Controller personal data except as necessary to maintain or provide the HPE Cloud Volume Services, or as necessary to comply with the law or a binding order of a governmental body.
3. Processor will not (a) disclose Controller personal data to any government or third party (other than Processor affiliates and service providers) or (b) store Controller personal data in a region other than the Processor regions selected by Controller, except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body, Processor will give Controller notice of any legal requirement or order referred to in this section.

4. Processor will only use Controller account information in accordance with the applicable Processor privacy terms and Controller consent to such use.
5. Processor may use affiliates and third-party service providers to perform the services. Controller understands, agrees, and authorizes Processor to share access to Controller personal data with such third parties to maintain and provide the services, and consistent with the purposes described in the Processor privacy terms.
6. Processor will provide Controller with a list of current service providers performing the services.
7. 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.
8. 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 employees and contractors are contractually bound to maintain the confidence of Controller personal data and comply with applicable Processor policies, 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.
9. In the event 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:
 - 9.1. 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.
 - 9.2. 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.

V1 a00061664ENW - V2 a50009388ENW

HEWLETT PACKARD ENTERPRISE

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

