

HPE GreenLake edge-to-cloud platform SaaS

Annex II: Description of the processing

1.	Description of processing	<p>HPE GreenLake platform is a unified cloud platform that enables IT users and partners to onboard and manage Processor services including compute, data storage, and networking through a common management console and deliver them in an as-a-service offering. The basic building blocks for the common services are authentication, authorization, Controller, and user on-boarding, device management, subscription management, and such. Provisioning Services: The information gathered and stored by the product is the minimum required to help ensure secure access to the portal and is essential to performing its function. The audit logs about a user will be automatically purged after 90 days. Support Services: Access to the Controller environment and data for troubleshooting is provided to Processor’s HPE GreenLake platform support services based on Controller agreements and permissions.</p>
2.	Type of personal data processed	<p>Personal data collected as part of network management and related applications include:</p> <ul style="list-style-type: none"> a. Device IP b. Name c. User name d. Email e. Address f. Phone
3.	Categories of personal data processed	<p>Controller’s client, end user, employee, contractor, temporary worker, and MSP, and channel partners.</p>
4.	Duration of processing	<p>The audit logs about a user will be automatically purged after 90 days.</p>
5.	Technical & Organizational Measures	<p>Processor shall maintain the information and physical security program for the protection of Controllerpersonal data as detailed in Annex III below.</p>

HPE GreenLake edge-to-cloud platform SaaS

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

Product Security Features:

1. Physical Security

HPE GreenLake platform is hosted in the most widely adopted infrastructure-as-a-service (IaaS) platform — Amazon Web Services (AWS) — that offers the most comprehensive security and compliance features. AWS has put in place security measures around the critical areas including perimeter, infrastructure, data, and environment layers.

2. Network Security

Processor network security helps ensure that the physical and virtual network on which the application and data resides is secure. Processor uses services and tools that the IaaS provider offers and some third-party solutions to make sure Processor production environment is as secure as it can be from external threats and internal vulnerabilities. Processor's HPE GreenLake platform operates separate instances of internal and production environments. The internal environment is focused on development and testing while the production environment is solely reserved for Controller. Having this physical and logical separation of Processor production environment from other running instances helps Processor offer the most secure software deployment to Controller and helps ensure their data is confined to one environment. Processor provides (i) reasonable assistance 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.

3. Application Architecture and Security

The traffic that is exchanged between the Processor HPE GreenLake platform application and the outside world is done using HTTPS over TLS. All traffic flow is encrypted using AES encryption technology. Different application tiers such as web, app, and database are designed to operate in an allow list framework. Only necessary and required communication paths are allowed between tiers. Each instance within a tier is protected by firewall rules to prevent any unauthorized or malicious access. Application is scanned for common vulnerabilities and exposures (CVEs), and Open Web Application Security Project (OWASP) security bugs and credible bugs are fixed.

4. Data Security

The data exchange between the Processor's HPE GreenLake platform and applications and users happens using HTTPS. Personal data at rest is encrypted. Personal data backup occurs regularly, and backup data is stored redundantly. From an organizational perspective, Processor has a DevOps team that manages the security and operational aspects of the app.

5. Geographic Availability

Processor's HPE GreenLake platform is currently available in the US West (Oregon) Region. Processor's HPE GreenLake platform is deployed on clusters in AWS US West Region, with AWS providing the compute and storage infrastructure. The following table provides a list of Processor's HPE GreenLake platform clusters and the supporting AWS Regions:

HPE GreenLake Platform Clusters and Supporting AWS Regions		
US-West-2	US West (Oregon)	Current URL is common.cloud.hpe.com
US-East	US East (Ohio)	

Processor's HPE GreenLake platform stores account information (for example, email addresses, name, phone number provided during the account registration) for account registration, administration, service access, and audit log. See Processor Privacy Statement (hpe.com/us/en/legal/privacy.html) for details on how Processor's HPE GreenLake platform processes personal data as a data controller.

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.

a50006106ENW - Annex a50009451ENW

HEWLETT PACKARD ENTERPRISE

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

