

# HPE Networking Instant On

## Annex II: Description of the processing

1.	Description of processing	<p>Processor's HPE Networking Instant On is a networking solution for small and medium sized businesses and enterprises. The solution offers a mobile app and web portal for configuration, monitoring, reporting, and troubleshooting purposes. The mobile app and web portal are driven by a cloud platform that maintains information about the Controller's network and deployment to enable the offered management and other services. Processor and its affiliates will (i) have access to Controller personal data hosted in Processor's cloud platform as part of the operation of the product and (ii) during product support and maintenance services. Product operation: All data (personal and non-personal) that is stored in the cloud platform to enable product operation including product functionality, configuration, monitoring, reporting, and troubleshooting services will be available for the purpose of enabling product operation. Support and maintenance services: All data (personal and non-personal) is accessible to the HPE Networking Instant On technical support team only for the purpose of helping a Controller through a support and/or maintenance ticket(s).</p>
2.	Type of personal data processed	<p>HPE Networking Instant On knows the following user information:</p> <ul style="list-style-type: none"> <li>a. User's email address</li> <li>b. User's country information</li> <li>c. MAC address of Access Points</li> <li>d. IP address of Access Points</li> <li>e. MAC address of connected wireless clients on-site</li> <li>f. IP address of connected wireless clients on-site</li> <li>g. Application visibility and counters: Keep traffic usage on a per client, with coarse visibility on applications or website category being accessed.</li> </ul>
3.	Categories of personal data processed	All users who access Controller's wireless network
4.	Duration of processing	Processor shall process Controller personal data for the duration of the applicable transaction document.
5.	Technical & Organizational Measures	Processor shall maintain the information and physical security program for the protection of Controller personal data as detailed in Annex III below.

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

1. 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.
2. Processor 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.
3. 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:
  - a. 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. Notice shall be provided to Processor Security Operations Center via email at [security@hpe.com](mailto:security@hpe.com).
  - b. 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.
4. Processor applications are hosted on AWS. AWS data center(s) security certifications can be found at [aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/](https://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/).

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.

a50009459ENW, Rev. 3

HEWLETT PACKARD ENTERPRISE

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

