

HPE Data Privacy and Security Addendum

This Data Privacy and Security Addendum (“DPSA”) is made a part of the Agreement (defined below) and governs the privacy and security of Personal Data (defined below) processed in connection with the Services (defined below). If there is a conflict between the Agreement and this DPSA, the terms of this DPSA will control.

1. Definitions

“**Affiliate**” means an entity that directly or indirectly, controls, is controlled by, or is under common control with a party. “Control,” “controlled by,” and “under common control” mean ownership, either direct or indirect, of more than fifty percent of the equity interest entitled to vote for the election of directors or equivalent governing body. An entity is considered an Affiliate of a party only for so long as such entity continues to meet the foregoing definition.

“**Agreement**” means the agreement for the provision of Services between HPE and Customer, or, if no agreement exists, HPE’s standard terms and conditions.

“**Applicable Laws**” means applicable local, state, and federal laws, rules, regulations, ordinances, codes, orders, and legally binding decrees, as amended and replaced from time to time, of all governments or agencies of domestic or foreign jurisdictions, that are applicable to the Customer Personal Data.

“**BCR-P**” means Binding Corporate Rules for Processors.

“**Confidential Information**” has the meaning given to it in the Agreement.

“**Controller**” means the entity that determines the purposes and means of the Processing of Personal Data, including as applicable, any “Business” as that term is defined under Applicable Laws.

“**Customer Personal Data**” means the Personal Data specified in the Supplemental Privacy Information that HPE Processes on behalf of Customer in the context of providing Services.

“**Data Subject**” means an identifiable person whose Personal Data is Processed.

“**HPE**” means the contracting Hewlett Packard Enterprise group company.

“**HPE Entity**” means Hewlett Packard Enterprise Company or the Affiliate(s) participating in Hewlett Packard Enterprise’s BCR-P, as indicated here: <https://www.hpe.com/us/en/privacy/binding-corporate-rules.html>.

“**Personal Data**” has the meaning given to that term under Applicable Laws and includes “Personal Information” as that term is defined under Applicable Laws.

“**Processor**” means an entity that Processes Personal Data on behalf of a Controller, including as applicable, any “Service Provider” as that term is defined under Applicable Laws.

“**Security Breach**” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, exfiltration, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

“**Sensitive Personal Data**” means Personal Data defined as “special category” or “sensitive” by Applicable Laws.

“**Services**” means the services provided by HPE to Customer under the Agreement.

“**Subprocessor**” means an entity engaged by HPE or its Affiliate to Process Customer Personal Data.

“**Supplemental Privacy Information**” means the information within Annexes I, II and III, and the lists of Subprocessors for the relevant Services, located at [hpe.com/us/en/legal/customer-privacy.html](https://www.hpe.com/us/en/legal/customer-privacy.html).

Capitalized terms that are not otherwise defined have the meanings set forth in Applicable Laws.

2. Appointment and Instructions

- 2.1 Customer acts as Controller and HPE acts as Processor of Customer Personal Data. Customer authorizes HPE to Process Customer Personal Data to provide the Services, which includes Processing Customer Personal Data as reasonably necessary for the internal purposes of improving the Services and enhancing the user experience. Details of the Processing, including the purposes, duration, the types and categories of Personal Data, and other information are in the Supplemental Privacy Information. HPE may Process Customer Personal Data if required under Applicable Laws and HPE shall inform Customer of such a requirement unless HPE is prohibited by law. If HPE believes that an instruction from Customer will violate Applicable Laws, then HPE shall promptly notify Customer. Any additional instructions must be mutually agreed upon pursuant to the terms of the Agreement and may be subject to additional fees or expenses.
- 2.2 If Customer uses the Services to Process any Personal Data not expressly covered by this DPSA, Customer acts at its own risk and HPE is not responsible for any non-compliance with this DPSA.

3. Compliance with Applicable Laws

- 3.1 The parties shall comply with their obligations under Applicable Laws. HPE shall promptly notify Customer if it determines that it can no longer meet its obligations under Applicable Laws. To the extent that compliance with a change in Applicable Laws requires a change to the scope of the Services, the parties shall, acting reasonably, agree to an appropriate amendment to the Agreement and the payment of any reasonable costs associated with such change. Customer has provided all required notices and obtained all required permissions under Applicable Laws to provide HPE with the Customer Personal Data, and to permit the Personal Data to be lawfully Processed by HPE and its Subprocessors under the Agreement.
- 3.2 In the event that HPE receives a regulatory request, order, or other binding decision from a competent authority that requires amendments to this DPSA or any changes to the Processing of Customer Personal Data ("Regulatory Request"), HPE and Customer shall, within a reasonable time after receiving the Regulatory Request, work in good faith towards a plan to address the Regulatory Request. A time frame for reviewing the Regulatory Request and preparing a compliance review plan will be agreed upon between the parties, taking into account the requirements of Applicable Laws.
- 3.3 If HPE Processes Protected Health Information on behalf of a Covered Entity or Business Associate (each as defined under the Health Insurance Portability and Accountability Act), then the terms of HPE's Business Associate Agreement within the Supplemental Privacy Information apply to such Processing.

4. Security & Security Breach

- 4.1 HPE shall implement the appropriate physical, technical, and organizational measures described in the Supplemental Privacy Information to help protect Customer Personal Data. HPE may change the specific physical, technical and organizational measures to account for enhanced technologies; provided that HPE does not diminish the level of protection.
- 4.2 Upon request, HPE shall make available to Customer information necessary to demonstrate compliance with the DPSA and Applicable Laws. For such purposes, HPE agrees to respond, no more than once every 12 months and subject to thirty (30) days' prior written notice, to a reasonable information security questionnaire concerning security practices specific to the Services provided. HPE shall, upon request, make available to Customer summary information or certifications (e.g., ISO 27001, SOC reports), where available for the Services in scope. If the foregoing is insufficient to demonstrate HPE's compliance with the DPSA and Applicable Laws, Customer is entitled to, no more than once every 12 months, monitor HPE's compliance with the DPSA and Applicable Laws through reasonable measures, including remote audits (e.g., via MS Teams or Zoom), limited to the Services provided under the Agreement. Such audits may be carried out on HPE's premises only where required by Applicable Laws. Any audit or assessment will be conducted at Customer's expense and during business hours, in a manner that minimizes disruption to HPE's operations, using appropriate and accepted control standards or frameworks and audit processes. Any third party engaged by Customer to conduct an audit must: (i) be pre-approved by HPE (such approval not to be unreasonably withheld); and (ii) enter into a confidentiality agreement reasonably acceptable to HPE. Any information obtained by Customer under this subsection shall be deemed HPE's Confidential Information.

- 4.3 HPE will notify Customer, without undue delay, of any Security Breach impacting Customer Personal Data, including providing information reasonably required for Customer to comply with Applicable Laws. If Customer becomes aware of a Security Breach that affects the Services, Customer shall promptly notify HPE of the scope of the Security Breach. Notifications shall be made to security@hpe.com or such other contact designated by HPE in writing.

5. Confidentiality and Disclosure

- 5.1 HPE shall put procedures in place that are designed to ensure that all persons acting under its authority who are entrusted with the Processing of Customer Personal Data: (i) have committed themselves in writing to keep such data confidential; or (ii) are under an appropriate statutory obligation of confidentiality. HPE shall ensure that access to Customer Personal Data is limited to those persons under its authority that have a need to know.
- 5.2 To the extent permitted by law, HPE shall notify Customer promptly in writing of any subpoena or other legal order issued by a government authority requiring access to or disclosure of Customer Personal Data. Such notice will describe the Customer Personal Data to be disclosed and the identity of the third party requiring such disclosure. HPE shall reasonably cooperate with Customer in its efforts to seek a protective order or other appropriate remedy or, in the event such protective order or other remedy is not obtained, to use reasonable efforts to obtain assurances that confidential treatment will be accorded to such Customer Personal Data.

6. Subprocessing

- 6.1 Customer authorizes HPE to engage affiliated and unaffiliated Subprocessors to perform some or all HPE's obligations under the Agreement to the extent necessary to provide the Services. The approved Subprocessors applicable to the Services and location of Processing can be found within the Supplemental Privacy Information or as otherwise provided to Customer. Customer will subscribe to HPE's notification tool as described in the Supplemental Privacy Information. Customer may object to the appointment or replacement of a Subprocessor within fourteen days of notification by HPE, and such objections must be based on documented evidence that establishes that the Subprocessor does not or cannot comply with this DPSA or Applicable Laws. In such an event, the parties shall use reasonable endeavors to resolve Customer's objection, and if the parties fail to agree on an amicable resolution to the proposed Subprocessor change, HPE may terminate the affected Services without liability.
- 6.2 HPE shall execute enforceable, written contracts with Subprocessors that require the Subprocessors to abide by terms no less protective than those in this DPSA that are applicable to the Processing and protection of Customer Personal Data. HPE remains responsible for the acts and omissions of its Subprocessors that result in a breach of this DPSA.

7. Data Transfers

- 7.1 Customer agrees that HPE may Process Customer Personal Data in a country outside of the country where the Customer Personal Data originated. The parties will rely on the BCR-P where an international data transfer involves an HPE Entity and is made from the EEA or Switzerland, or once approved by the relevant authority, from the UK. HPE may transfer Customer Personal Data to an HPE Entity in any country in accordance with the BCR-P. The BCR-P includes an intercompany agreement and applicable policies and procedures that form HPE's Binding Corporate Rules for Processors that apply to HPE's Processing of Customer Personal Data. Upon request, a copy of the documentation comprising the BCR-P is available to Customer and is to be considered HPE's Confidential Information. Where the BCR-P applies, applicable third-party beneficiary rights may be enforced against HPE.
- 7.2 Where the transfer involves Sensitive Personal Data, Customer warrants that Data Subjects have been informed: (i) that their Personal Data may be transmitted to another country; and (ii) of the existence of Processors located outside their home country and of the legal or contractual mechanisms relied upon to support such transfers, as required by Applicable Laws. Customer shall make available to Data Subjects a link to any notices or information required under those laws, including, as applicable, a BCR Rights Notice.
- 7.3 To the extent that the Processing of Customer Personal Data by HPE involves the transfer of Customer Personal Data from the EEA/EU, the UK, Switzerland, Brazil, or Saudi Arabia to another country or territory that has not received an adequacy decision or otherwise been approved by the relevant authorities, and other than where the BCR-P applies, the Processing will also be subject to the applicable Standard Contractual Clauses within the Supplemental Privacy Information. To the extent there is a conflict between the terms of the Standard Contractual Clauses and the DPSA, the Standard Contractual Clauses will prevail.

8. Additional Restrictions on Processing of US Customer Personal Data

To the extent required under Applicable Laws, HPE: (i) shall not Sell or Share Customer Personal Data; (ii) shall not retain, use, or disclose Customer Personal Data for any purpose, including any commercial purpose, other than for the business purposes set forth in this DPSA and the Agreement, or as otherwise permitted by Applicable Laws; (iii) shall not retain, use, or disclose Customer Personal Data outside of the direct business relationship between HPE and Customer, unless permitted by Applicable Laws; (iv) shall not combine Customer Personal Data that it receives from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another person(s), or collects from its own interaction with the Data Subject except as permitted by Applicable Laws; and (v) grants Customer the right, upon notice, and consistent with the terms in this DPSA, to take reasonable and appropriate steps to stop and remediate HPE's unauthorized use of Customer Personal Data as permitted by Applicable Laws.

9. Providing Customer Assistance

At Customer's request and subject to additional fees, HPE shall provide reasonable assistance with: (i) requests from Data Subjects seeking to exercise their privacy rights under Applicable Laws as described in HPE's Privacy Statement; and (ii) carrying out a privacy impact assessment, including a prior consultation with supervisory authorities.

10. Data Retrieval and Destruction

If Customer cannot access Customer Personal Data after the cessation of the Services, HPE shall, in accordance with Customer's written instructions and at Customer's election, return or securely destroy the Customer Personal Data and, upon request, provide written confirmation. HPE may retain Customer Personal Data to the extent and for the duration required by Applicable Laws. If HPE is unable to delete or return Customer Personal Data due to Applicable Laws, HPE shall, to the extent permitted by law, inform Customer of that obligation.

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.

a50016070ENW

HEWLETT PACKARD ENTERPRISE

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

