

HPE Data Sanitization Services

附錄 II：處理說明

1.	處理說明	在提供現場 Data Sanitization Services 的過程中，處理者會將控制者所控制的裝置與處理者設備連接，使處理者設備得以覆寫控制者裝置上存在的任何資料，以此完成資料的清除。此資料可能包括儲存在裝置上的控制者個人資料。
2.	處理的個人資料類型	處理的個人資料類型將取決於控制者儲存在裝置上的資料，其中可能包含敏感的個人資料。
3.	處理的個人資料類別	凡其個人資料是由控制者儲存在控制者裝置上的，則相關資料主體皆在處理範圍內，包括但不限於控制者的客戶、一般使用者、員工、承包商和臨時工作者。
4.	處理期間	處理者應在本協議和/或任何適用的交易文件期間處理控制者的個人資料。
5.	技術和組織措施	處理者應維護資訊和實體安全計畫，以保護控制者的個人資料，如下文附錄 III 中詳述。

HPE Data Sanitization Services

附錄 III：技術和組織措施，包括確保資料安全的技術和組織措施

1. Data Sanitization Services 不涉及跨國資料轉送。
2. 處理者基礎架構在合理範圍內具有最新版本的系統安全軟體，其中可能包括主機防火牆、防毒軟體以及最新的修補程式和病毒定義檔。處理者維護涉及基礎架構的事件記錄，包括維護入侵偵測系統以用於監控、偵測及回報濫用情況、可疑活動、未授權的使用者及其他安全風險。
3. 員工和承包商接受處理者隱私權和安全政策的訓練，並瞭解自己在隱私權和安全實務做法方面的責任。處理者的員工和承包商受合約之約束，必須維護控制者個人資料的機密性，並遵守與處理控制者個人資料相關的適用處理者政策、標準或要求。未能遵守這些政策、標準或要求將受到調查，可能會導致紀律處分，嚴重者包括終止與處理者的僱用關係或任何合作關係。
4. 若處理者確認存在安全漏洞，導致控制者個人資料遭到意外或非法破壞、遺失、更改或未經授權披露或存取（「安全事件」），處理者將：
 - 4.1 立即向控制者報告安全事件。處理者將向控制者提供有關安全事件狀態的更新，直到問題得到解決為止。報告內容包括但不限於對安全事件的描述、採取的行動和矯正行動方案。如果控制者發現影響服務的安全事件，控制者應立即通知處理者，並告知處理者安全事件的影響範圍。

4.2 應控制者的要求並由其承擔相關費用·(i) 向控制者提供合理之協助·以便根據適用於控制者的隱私權法向主管監管機構通報安全漏洞；(ii) 在資料外洩可能對個人權利和自由造成高風險時·向控制者提供合理之協助·以將資料外洩情況傳達給資料主體。

造訪 [HPE.com](https://www.hpe.com)

[立即線上交談](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. 本文件所含資訊如有變更·恕不另行通知·HPE 產品與服務的唯一保固詳細記載於此類產品與服務隨附的明示保固聲明中·本文件中的任何資訊均不應解讀為構成額外的保固·HPE 對本文件中的技術·編輯錯誤或遺漏概不負責。

a00046994ZHT - 附錄 a50009391ZHT

HEWLETT PACKARD ENTERPRISE

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

