

# HPE Data Sanitization Services

## Allegato II: Descrizione del trattamento dei dati

1. Descrizione del trattamento dei dati	Nell'ambito della fornitura in loco dei servizi Data Sanitization, il Responsabile del trattamento collegherà il dispositivo controllato dal Titolare del trattamento a un'appliance del Responsabile del trattamento che sovrascriverà gli eventuali dati presenti sul dispositivo Titolare del trattamento per cancellarli. Tali dati possono includere i dati personali del Titolare conservati sul dispositivo.
2. Tipo di dati personali trattati	Il tipo di dati personali trattati dipende dai dati che il Titolare del trattamento ha conservato sul dispositivo e può includere dati personali sensibili.
3. Categorie di dati personali trattati	Qualsiasi interessato i cui dati personali siano conservati dal Titolare del trattamento sul dispositivo del Titolare, compresi, a titolo esemplificativo, i clienti del Titolare, gli utenti finali, i dipendenti, i collaboratori esterni e i lavoratori temporanei.
4. Durata del trattamento	Il Responsabile tratta i dati personali del Titolare per la durata del Contratto e/o di qualsiasi documento di transazione applicabile.
5. Misure tecniche e organizzative	Il Responsabile del trattamento mantiene il programma di sicurezza informatica e fisica per la protezione dei dati personali del Titolare, come specificato nell'Allegato III di seguito.

## HPE Data Sanitization Services

### Allegato III: Misure tecniche e organizzative, comprese le misure tecniche e organizzative a garanzia della sicurezza dei dati

1. Non verranno effettuati trasferimenti internazionali di dati nell'ambito dei servizi Data Sanitization.
2. L'infrastruttura del Responsabile dispone di versioni adeguatamente aggiornate del software di sicurezza del sistema, che possono includere firewall dell'host, protezione antivirus e definizioni di patch e virus aggiornate. Il Responsabile conserva i registri degli eventi che coinvolgono l'infrastruttura, compresi i sistemi di rilevamento delle intrusioni per monitorare, rilevare e segnalare modelli di abuso, attività sospette, utenti non autorizzati e altri rischi per la sicurezza.
3. I dipendenti e i collaboratori esterni sono formati sulle politiche del Responsabile in materia di privacy e sicurezza e resi consapevoli delle loro responsabilità in merito alle pratiche di privacy e sicurezza. I dipendenti e i collaboratori esterni del Responsabile del trattamento sono tenuti per contratto a mantenere la riservatezza

dei dati personali del Titolare e a rispettare le politiche, gli standard o i requisiti del Responsabile applicabili in relazione al trattamento dei dati personali del Titolare. La mancata osservanza di tali politiche, standard o requisiti sarà soggetta a indagini che potrebbero comportare azioni disciplinari fino alla cessazione del rapporto di lavoro o dell'incarico da parte del Responsabile.

4. Nel caso in cui il Responsabile confermi una violazione della sicurezza che comporti la distruzione accidentale o illegale, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali del Titolare ("Incidente di sicurezza"), il Responsabile provvede a:
  - 4.1 Informare dell'Incidente di sicurezza il Titolare senza ingiustificato ritardo. Il Responsabile fornisce al Titolare aggiornamenti sullo stato dell'Incidente di sicurezza fino a quando la questione sarà stata risolta. I report includono, a titolo esemplificativo, una descrizione dell'Incidente di sicurezza, le azioni intraprese e i piani di correzione. Qualora il Titolare venga a conoscenza di un Incidente di sicurezza che riguardi i servizi, il Titolare riferisce tempestivamente l'accaduto al Responsabile e lo informa sulla portata dell'Incidente di sicurezza.
  - 4.2 Su richiesta e a spese del Titolare del trattamento, (i) fornisce un'opportuna assistenza al Titolare nel notificare una violazione della sicurezza all'autorità di vigilanza competente ai sensi delle leggi sulla privacy applicabili al Titolare; e (ii) fornisce un'opportuna assistenza al Titolare nel comunicare una violazione dei dati agli interessati nei casi in cui la violazione dei dati possa comportare un rischio elevato per i diritti e le libertà delle persone.

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

[Avvia chat](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i prodotti e i servizi Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni o errori tecnici o editoriali contenuti nel presente documento.

a00046994ITE - Allegato a50009391ITE

HEWLETT PACKARD ENTERPRISE

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

