PRIVACY POLICY - KEYCRYPTA ULTIMO AGGIORNAMENTO: Marzo 2026

Introduzione Questa informativa spiega come KeyCrypta protegge la privacy degli utenti del suo software di gestione password. La tutela dei dati personali è garantita nel rispetto delle normative applicabili (es. GDPR/UE, CCPA-CPRA/USA, LGPD/BR, PIPEDA/CA, APP/AU, POPIA/ZA, APPI/JP).

1. Titolare del trattamento

KeyCrypta ("Licenziante"). Contatto privacy: privacy@keycrypta.com Per attivazioni/cambio hardware: info@keycrypta.com Sito: www.keycrypta.com

2. Ambito di applicazione e operatività

Il Software opera offline. Le uniche comunicazioni verso l'esterno possono avvenire: (i) per l'attivazione/ri-attivazione della licenza se l'utente invia volontariamente l'UUID; (ii) per la funzione opzionale "Verifica Violazione Password" (vedi sotto). Nessun dato viene trasmesso o archiviato al di fuori del dispositivo, salvo quanto sopra indicato.

3. Dati trattati localmente

- Credenziali e note, archiviate cifrate sul dispositivo su cui è utilizzato KeyCrypta (Windows 10 o Windows 11). Informazioni sul sistema operativo

(edizione /versione /build) possono essere rilevate e memorizzate localmente per finalità di compatibilità, diagnostica e audit; non sono trasmesse all'esterno. Esempio: Windows-11-10.0.22631-SP0.

- UUID del dispositivo, memorizzato cifrato solo per gestione licenza.

- (Se presenti) Log locali (data/ora, esito login, operazioni principali), salvati cifrati per sicurezza e audit personale.

Nessuno di questi dati è trasmesso o condiviso automaticamente; possono essere trasmessi solo se l'utente genera e invia volontariamente una richiesta di attivazione / ri-attivazione / rinnovo (ad es. via e-mail o tramite il sito www.keycrypta.com), che può includere UUID e informazioni di sistema necessarie alla gestione della licenza.

4. Funzione opzionale "Verifica Violazione Password"

L'utente può attivare un controllo online tramite "Have I Been Pwned". Meccanismo: la password è convertita in SHA-1 e vengono inviati solo i primi 5 caratteri dell'hash (k-anonymity). La verifica finale avviene localmente confrontando le risposte con l'hash completo. La funzione è disabilitata di default. Non inviamo né memorizziamo la password in chiaro; non inviamo l'hash completo: viene trasmesso solo il prefisso di 5 caratteri (k-anonymity) e la verifica finale avviene localmente.

5. Licenza e UUID

L'UUID (identificatore hardware esposto da BIOS/UEFI) è usato esclusivamente per associare la licenza al dispositivo; di per sé non include nome/cognome né contenuti della cassaforte. L'UUID non è trasmesso automaticamente: può essere inviato dall'utente via e-mail o tramite la pagina web di www.keycrypta.com esclusivamente ai fini di attivazione, ri-attivazione o cambio hardware/PC, su iniziativa dell'utente o su richiesta del Licenziante accettata dall'utente.

6. Finalità del trattamento

- Consentire il corretto funzionamento del Software.
- Gestire e verificare l'attivazione/ri-attivazione della licenza.
- Effettuare controlli di sicurezza anonimi tramite Have I Been Pwned (solo se attivati dall'utente).
- (Se presenti) Migliorare la sicurezza individuale tramite log solo locali.

7. Base giuridica del trattamento

- Esecuzione del contratto: operazioni strettamente necessarie al funzionamento del Software e alla gestione della licenza.
- Consenso esplicito: funzionalità opzionali (es. verifica password).

8. Modalità di trattamento e conservazione

I dati generati dall'uso del Software sono memorizzati unicamente in locale ed è l'utente a detenerne il controllo (creazione, modifica, esportazione, cancellazione). Non comunichiamo dati personali a terzi, salvo i dati anonimi della verifica password come descritto. I dati sono conservati per il tempo strettamente necessario alle finalità indicate. (Se presenti) i log possono essere eliminati dall'utente in qualunque momento.

9. Diritti degli utenti

L'utente può accedere, rettificare, cancellare i dati, limitarne/opporne il trattamento, revocare il consenso ove previsto e proporre reclamo all'autorità competente (es. Garante Privacy in Italia o l'equivalente all'estero). Per esercitare i diritti: privacy@keycrypta.com.

10. Trasferimenti internazionali

Il Software non trasferisce dati personali al di fuori del Paese dell'utente, salvo:

- chiamate limitate (k-anonymity) a Have I Been Pwned (funzione disattivata per impostazione predefinita, attivabile solo dal Pannello Amministratore e su

specifica richiesta dell'utente; KeyCrypta funziona anche senza tale verifica, che ha finalità informativa di controllo su possibili password compromesse);

- eventuale invio volontario dell'UUID per attivazione/ri-attivazione.

Eventuali trasferimenti saranno effettuati nel rispetto delle normative applicabili.

11. Misure di sicurezza

Adottiamo misure tecniche e organizzative adeguate, tra cui a titolo esemplificativo:

- cifratura autenticata dei dati (es. XChaCha20-Poly1305);
- derivazione robusta della password (es. Argon2id con parametri adeguati);
- controllo di integrità e firma digitale modulare; timeout di sessione;
- pulizia della clipboard; sovrascrittura sicura di RAM/file; controllo accessi (ACL) ai file sensibili;
- (se presente) modalità "panico" per cancellazione locale.

I dettagli possono evolvere con gli standard di settore.

12. Aggiornamenti della presente informativa

Potremo aggiornare questa informativa. Le modifiche saranno comunicate sul sito o in-app; quando richiesto dalla legge potrà essere richiesto un nuovo consenso o fornita ulteriore informativa. L'uso del Software dopo l'entrata in vigore delle modifiche implica la presa visione della versione aggiornata.