wasabi

Conformità al GDPR con Wasabi

Indice dei contenuti

Executive Overview

Wasabi è un servizio di cloud storage veloce e conveniente. Aziende e istituzioni utilizzano l'hot cloud storage di Wasabi per scopi differenti, tra cui l'archiviazione primaria di dati e contenuti delle applicazioni, l'archiviazione secondaria per il backup o il disaster recovery, e l'archiviazione per la conservazione a lungo termine di dati e documenti.

Il Regolamento generale sulla protezione dei dati (GDPR) dell'UE, entrato in vigore nel Maggio 2018, impone requisiti rigorosi sulle modalità di gestione e protezione dei dati personali

Le aziende soggette al GDPR possono utilizzare Wasabi per archiviare e conservare i dati personali. Wasabi utilizza le migliori pratiche e tecnologie di sicurezza per garantire la sicurezza fisica delle proprie strutture e per mantenere la privacy e l'integrità dei dati personali. Inoltre, l'Accordo sui termini di utilizzo di Wasabi garantisce che i clienti di Wasabi (“responsabili del trattamento dei dati” ai sensi del GDPR) mantengano la proprietà esclusiva dei dati elettronici, come richiesto dal GDPR.

Questo white paper fornisce una breve panoramica sull'uso del servizio Wasabi alla luce del GDPR.

Introduzione - Panoramica sul GDPR

Il GDPR è stato emanato nel 2016 per rafforzare e armonizzare la protezione dei dati personali all'interno dell'Unione Europea. Il suo scopo è quello di fornire ai cittadini un maggiore controllo sui loro dati personali e di migliorare lo scambio di informazioni all'interno dell'UE. Il GDPR regola anche l'esportazione di dati personali al di fuori dell'UE (ma in questo caso non richiede che i dati personali siano conservati all'interno dell'UE).

Il GDPR è entrato in vigore il 25 Maggio 2018, sostituendo la direttiva europea sulla protezione dei dati (95/46/CE). Il nuovo regolamento si applica a qualsiasi azienda o ente presente nell'UE o che offre beni o servizi nell'UE.

I termini rilevanti per il GDPR sono:

- Titolare del trattamento dei dati - un'azienda o ente che raccoglie o fornisce dati relativi a residenti nell'UE (ad esempio, un cliente Wasabi).
- Responsabile del trattamento dei dati - un'azienda o ente che elabora i dati per conto di un responsabile del trattamento dei dati (ad esempio, un provider di cloud come Wasabi).
- Soggetto interessato - una persona residente nell'Unione Europea.
- Dati personali - qualsiasi informazione di identificazione personale relativa a un soggetto interessato (ad esempio, nome, numero di identificazione, dati di localizzazione, identità online ecc...).

Implicazioni per la privacy e la sicurezza dei dati del GDPR

Il GDPR impone regole ferree in materia di privacy e sicurezza dei dati sia per i titolari che per i responsabili del trattamento. Impone, ad esempio, garanzie adeguate per proteggere la privacy dei dati personali e definisce regole in merito al consenso per la divulgazione dei dati personali. Il GDPR garantisce inoltre alle persone il diritto di esaminare, modificare, correggere e cancellare i dati personali.

Tra le principali disposizioni del GDPR in materia di privacy e sicurezza dei dati ci sono:

- Gli articoli 15, 16 e 17 - diritti di accesso, rettifica e cancellazione - garantiscono agli interessati uno stretto controllo sui propri dati personali.
- Articolo 20 - diritto alla portabilità dei dati - garantisce alle persone il diritto di trasferire i dati personali da un sistema elettronico di elaborazione a un altro.
- Articolo 25 - protezione dei dati “by design” e “by default” - impone ai titolari del trattamento di implementare adeguate misure tecniche e organizzative per salvaguardare i dati personali.
- Articolo 32 - sicurezza del trattamento - richiede la “pseudonimizzazione” e la crittografia dei dati personali.
- Articoli 33 e 34 - notifica di una violazione dei dati personali - impone ai titolari del trattamento di notificare alle autorità di vigilanza e agli interessati se avviene un data leak o data breach.

Panoramica di Wasabi Hot Cloud Storage

Wasabi hot cloud storage è un servizio di archiviazione in cloud conveniente, veloce, affidabile e conforme al GDPR.
A differenza dei servizi di storagein cloud tradizionali, che presentano livelli di archiviazione confusi e un sistema di prezzie licenze molto complesso, Wasabi è intuitivo e molto semplice da implementare così come molto conveniente da scalare.
Le aziende e le istituzioni possono utilizzare Wasabi per:

- Archiviazione primaria a low-cost per applicazioni on-premise o in cloud.
- Storage secondario economico per il backup, il disaster recovery in cloud o le iniziative di migrazione dei dati.
- Archiviazione conveniente e affidabile per la conservazione dei dati a lungo termine.

Conformità al GDPR con Wasabi

Il servizio di cloud storage Wasabi è progettato per garantire la privacy e l'integrità dei dati personali. Il servizio è costruito e gestito secondo le migliori pratiche e gli standard di sicurezza, in conformità con quanto previsto dal GDPR.

Wasabi adotta un approccio di “defense-in-depth”, impiegando più livelli di sicurezza per garantire la massima protezione dei dati in accordo con le previsioni del GDPR e le linee guida di “privacy by design” e “privacy by default”.Wasabi garantisce la sicurezza fisica dei propri data center, istituisce solidi controlli di autenticazione e autorizzazione per tutte le infrastrutture di computing, storage e networking in cloud e cripta i dati a riposo e in transito per salvaguardare i dati personali.

Sicurezza fisica

Il servizio Wasabi è ospitato in data center di primo livello, altamente sicure, completamente ridondanti e certificate per la conformità SOC 2 e ISO 27001.Ogni sito è presidiato 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, da personale di sicurezza in loco per proteggere i dati da ingressi non autorizzati. Le telecamere di sicurezza monitorano costantemente l'intera struttura, sia all'interno che all'esterno. Sono posizionati lettori biometrici e meccanismi di autenticazione a due fattori o superiori per garantire l'accesso all'edificio. Le strutture non sono contrassegnate, in modo da non attirare l'attenzione dall'esterno.

Architettura di rete sicura

Wasabi impiega elementi avanzati di sicurezza di rete, tra cui firewall e altri dispositivi di protezione del perimetro, per monitorare e controllare le comunicazioni interne ed esterne. Questi dispositivi di sicurezza del perimetro sono configurati per creare una separazione logica tra i dati dei diversi clienti e per regolare il flusso comunicativo tra reti così da impedire acccessi non autorizzati alle infrastrutture e ai servizi di Wasabi.

Privacy e sicurezza dei dati

Wasabi supporta una serie di funzionalità per la privacy e la sicurezza dei dati per prevenire la divulgazione non autorizzata di dati personali. Le funzioni di autenticazione degli utenti controllano strettamente l'accesso ai dati memorizzati. Le solide funzionalità di autenticazione degli utenti regolano strettamente gli accessi ai dati salvati. Le liste di controllo degli accessi (ACL) e le policy di amministrazione prestabilite garantiscono selettivamente le permissioni di accesso a utenti o gruppi di utenti. Wasabi cripta i dati a riposo e quelli in transito per evitare la perdita di dati.

Tutti i dati archiviati su Wasabi sono crittografati di default per proteggere i dati a riposo. Tutte le comunicazioni con Wasabi sono trasmesse tramite HTTPS per proteggere i dati in transito.

Registrazione degli accessi

Wasabi supporta registri dettagliati degli accessi allo storage per scopi di audit. I registri contengono informazioni su ogni richiesta di accesso: tipo di richiesta, dati riguardati dall'accesso e la data e l'ora in cui la richiesta è stata elaborata.

Durata e protezione dei dati

Wasabi garantisce una durabilità degli oggetti estremamente alta, del 99,999999999%,proteggendo i dati da guasti hardware e errori di archiviazione.

Portabilità e cancellazione dei dati

I clienti di Wasabi possono facilmente esportare i dati su un'altra piattaforma di archiviazione o cancellare i dati personali per conformarsi ai requisiti di portabilità e garanzia del diritto di cancellazione dei dati previsiti dal GDPR.

Proprietà e condivisione dei dati

L'accordo sui termini di utilizzo della piattaforma di archiviazione Wasabi garantisce al titolare del trattamento dei dati la proprietà e il controllo esclusivi dei dati archiviati. Secondo i termini dell'accordo, l'abbonato (il titolare del trattamento dei dati) mantiene la proprietà di tutti i dati dell'abbonato. Tutti i dati memorizzati su Wasabi rimangono di proprietà esclusiva e riservata dell'abbonato.

Responsabilità del cliente

I clienti Wasabi di solito si interfacciano con il servizio Wasabi utilizzando applicazioni di gestione dei file e strumenti di backup di terze parti. Per garantire la conformità al GDPR, il personale IT deve assicurarsi che gli strumenti e le applicazioni di gestione dello storage utilizzati siano configurati per godere delle funzioni di sicurezza offerte da Wasabi. Ad esempio, l'HTTPS deve essere abilitato per criptare i dati in transito. Inoltre, i clienti devono criptare e "pseudonimizzare" tutti i contenuti e i dati prima di caricarli su Wasabi. Le aziende IT devono anche assicurarsi di disporre di sistemi e pratiche di sicurezza solidi per salvaguardare altri elementi dei loro sistemi on-premises e cloud. Il servizio di archiviazione Wasabi è solitamente utilizzato come parte di una più ampia implementazione cloud pubblica o ibrida che include componenti di calcolo, archiviazione e rete.

Conclusioni

Il GDPR introduce nuovi requisiti di privacy e sicurezza dei dati per le aziende e gli enti che operano nell'Unione Europea. I pianificatori IT, i team InfoSec e i responsabili della conformità devono garantire che i loro sistemi e le loro pratiche siano conformi alle nuove normative. Il servizio di cloud storage di Wasabi garantisce la privacy e l'integrità dei dati personali in conformità alle previsioni del GDPR. Wasabi garantisce la sicurezza fisica dei propri data center, impiega solidi controlli di autenticazione e autorizzazione per laprotezione dell'infrastruttura e dei servizi e cripta i dati a riposo e in transito per impedire la divulgazione non autorizzata dei dati. Wasabi solitamente è utilizzato insieme ad altre piattaforme e servizi di calcolo, storage e networking. Le organizzazioni IT devono implementare sistemi e pratiche di sicurezza solidi in tutte le infrastrutture on-premises e in cloud per proteggere completamente i dati personali.

Informazioni aggiuntive

Per ulteriori informazioni sul GDPR e su Wasabi, consultare le seguenti risorse:

- Pagina web della Commissione europea sulla protezione dei dati
- Testo completo del GDPR dell'UE
- Per ulteriori informazioni sull' Informativa sulla privacy di Wasabi

Informazioni su Wasabi

Wasabi fornisce un servizio di hot storage in cloud semplice,conveniente e con costi sempre prevedibili per le aziende di tutto il mondo. Consente alle organizzazioni di archiviare e accedere istantaneamente una quantità illimitata di dati al 1/5 del prezzo della concorrenza, senza livelli di servizio complessi o spese di trasferimento imprevedibili. Consigliata da decine di migliaia di clienti in tutto il mondo, Wasabi è stata riconosciuta come una delle aziende tecnologiche più innovative e in più rapida crescita. Wasabi, creata dai co-fondatori di Carbonite e pionieri del cloud storage David Friend e Jeff Flowers, è un'azienda privata con sede a Boston.

wasabi
hot cloud storage

www.wasabi.com