White Paper

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

PER GLI AMMINISTRATORI IT, I DIRIGENTI E I PROPRIETARI DI MEDIE IMPRESE

Conformità per le SMB da una prospettiva di archiviazione

Cos'è il GDPR?

Il **Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation)** dell'Unione Europea intende rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini dell'Unione Europea.

Inoltre, affronta anche il tema dell'esportazione di dati personali al di fuori dell'UE. Le organizzazioni al di fuori della Unione Europea che trattano dati di cittadini dell'Unione Europea sono soggette al GDPR.

Lo scopo principale è di restituire ai cittadini e ai residenti il controllo sui relativi dati personali e di semplificare l'ambito normativo per le aziende internazionali unificando il regolamento all'interno della UE.

Il GDPR contiene principalmente informazioni sulle modalità di elaborazione dei dati personali e definisce i ruoli di un processore e di un controllore dei dati. Inoltre, include informazioni su come gestire la protezione dei dati per progetto e la privacy dei dati per default.

Il GDPR entrerà in vigore il 25 maggio 2018.

Implicazioni del GDPR

Le aziende di piccole e medie dimensioni (SMB) che trattano i dati dei cittadini della UE sono responsabili della protezione dei dati da loro archiviati.

I dati devono essere archiviati sistematicamente e protetti da furto o uso improprio.

Le SMB devono anche essere in grado di soddisfare i diritti del soggetto dei dati GDPR seguenti:

- **essere informato sull'elaborazione dei dati**
- **accedere ai propri dati**
- **modificare o eliminare i propri dati**
- **trasferire i propri dati a un'altra organizzazione**

La conservazione dei dati è un altro fattore importante. Alcuni tipi di dati devono essere eliminati trascorso un certo periodo di tempo, ad esempio, i dati personali raccolti in connessione con l'acquisto di un prodotto e della garanzia associata.

Inoltre, altri tipi di dati devono essere archiviati per un periodo minimo di tempo, ad esempio, alcuni dati finanziari.

In pratica, le SMB devono conoscere la posizione di archiviazione dei dati personali ed essere in grado di rispondere tempestivamente alle richieste di dati.

Le organizzazioni che non rispettano il GDPR incorrono in seri rischi, nel caso di importanti violazioni dei sistemi, ad esempio, nel caso di hacker che si appropriano del contenuto del database di un cliente.

Le sanzioni finanziari possono raggiungere un limite massimo di 20 milioni di Euro o il 4% del fatturato annuale, a seconda di quale sia maggiore.

Necessità di conformità al GDPR

La maggior parte delle organizzazione stanno facendo del loro meglio per soddisfare i requisiti del GDPR. Sono consapevoli delle implicazioni della violazione dei loro dati.

Tuttavia, alcune organizzazioni di piccole e medie dimensioni stanno adottando un approccio attendista.

Tali organizzazioni ritengono che il GDPR sia destinato e interessi solo grandi società che raccolgono e trattano grandi quantità di dati personali come social network, provider cloud o motori di ricerca.

Molte di queste organizzazioni sono in attesa di vedere cosa accade quando un'azienda simile viola la legislazione.

Questo approccio è potenzialmente dannoso poiché la minaccia di insolvenza o persino di chiusura come risultato delle sanzioni GDPR è molto reale.

Il GDPR si applica a tutte le aziende, indipendentemente dalle dimensioni e dal fatturato.

Protezione dei dati per progetto e per default

In base al mandato GDPR, le società devono garantire un approccio alla protezione dei dati per progetto e per default.

Ad alto livello, ciò significa che le società devono proteggere i propri sistemi e processi per garantire che i dati non vadano persi o siano facilmente soggetti ad atti di pirateria.

Ciò richiede che la protezione dei dati sia progettata nello sviluppo dei processi aziendali di prodotti e servizi.

Inoltre, richiede che vengano definite per default impostazioni di privacy ad alto livello e che le misure tecniche e procedurali per l'intero ciclo di vita di elaborazione dei dati siano conformi con il regolamento.

Infine, le organizzazioni sono tenute a implementare meccanismi che garantiscano l'elaborazione dei dati personali solo quando necessario per uno scopo specifico.

Protezione dei dati GDPR in pratica

La protezione dei dati per progetto e per default potrebbe avere un impatto diretto sulla soluzione di archiviazione dei dati in uso.

In base ai requisiti del GDPR, l'archiviazione dei dati deve essere di facile accesso e gestione nonché deve prevedere la progettazione della privacy e della protezione sin dalle sue fondamenta.

- Se si intende archiviare i dati in-house, la propria azienda sarà sia controllore dei dati che elaboratore dei dati. Di conseguenza, sarà completamente responsabile delle ripercussioni qualora questi dati siano soggetti ad atti di pirateria o violino il regolamento.

- Se si intende utilizzare una soluzione pubblica su cloud o di archiviazione ibrida, è responsabilità dell'azienda assicurare che tale soluzione e il provider di terze parti siano conformi al GDPR.

Se i dati personali sono archiviati in-house su un server, un dispositivo NAS o altri dispositivi, per assicurare la conformità al GDPR, è necessario incorporare le seguenti funzioni nel dispositivo di archiviazione:

- **Protezione tramite password:** i dispositivi e i file e/o le cartelle contenenti dati personali devono essere protetti da password. Devono essere accessibili solo agli utenti che dispongono dell'autorizzazione ad accedere e/o elaborare i dati.

- **Crittografia:** i dati devono essere sempre crittografati quando archiviati o trasferiti.

- **Protezione fisica da furto/perdita:** i dispositivi utilizzati per l'archiviazione dei dati devono disporre di protezione fisica come un lucchetto Kensington o chiavi per dispositivi NAS e unità disco rigido in un server o simili.

- **Software antivirus** per garantire che i dati non vengano infettati da malware come il ransomware.

- **Protezione tramite firewall**

- **Backup e ripristino:** i backup devono essere automatizzati ed eseguiti giornalmente in modo da poter recuperare le copie più recenti dei dati personali in caso di perdita dei dati.

Inoltre, sono previste altre misure aggiuntive che sono ugualmente importanti:

- Un dispositivo di archiviazione che fornisce ridondanza RAID e protegge da guasti dell'unità disco rigido evita tempi di inattività del sistema e perdite di dati.

- È preferibile una soluzione di archiviazione centralizzata anziché l'archiviazione locale su PC, laptop o unità disco rigido esterne o portatili. Tali dispositivi sono più soggetti a furto e ad accesso non autorizzato. Inoltre, è estremamente difficile controllare chi ha accesso a tali dispositivi e ai dati in essi presenti.

Sistema chiuso

Configurazione sicura

Crittografia dei dati

Password

Antivirus
(venduto separatamente per TS3000/3010 & TS5000/5010)

Backup, replica, failover e crittografia

Funzionalità antifurto
- Protezione software: autenticazione all'avvio
- Protezione antifurto fisica

Nozioni fondamentali del GDPR per le SMB

Sono previste alcune operazioni fondamentali per la sicurezza dell'archiviazione dei dati che le SMB devono effettuare per garantire la conformità al GDPR in relazione alla protezione dei dati personali.

Directory radice di archiviazione

La directory radice è simile al tronco di un albero da cui si estendono tutti gli altri rami. Se un hacker ottiene accesso a una directory radice, può nascondere virus e malware alla vista facendo apparire codice dannoso come file importanti che non verranno rilevati dal software antivirus.

Pertanto, i sistemi operativi NAS devono essere chiusi in modo che persino l'amministratore del sistema non possa accedervi. In questo modo, si chiudono saldamente eventuali punti di accesso sfruttati dagli hacker che normalmente utilizzano strumenti rootkit per accedere alle directory radice.

Impostazione sicura

Spesso, quando una società configura un sistema NAS e una connessione Internet, deve impostare l'account e abilitare l'accesso remoto. Per alcuni sistemi NAS, questa è una pratica standard.

Tuttavia, è anche un processo sfruttato dagli hacker per sottrarre i nomi utente e le password nel trasferimento dei dati fuori dalla rete aziendale e su Internet.

Crittografia avanzata

I dati archiviati sulle unità disco rigido possono essere soggetti a furto. La crittografia AES 256 dell'unità disco rigido, teoricamente inattaccabile, impedisce la lettura dei dati anche quando le unità vengono rimosse.

Buffalo TeraStation™, la soluzione NAS più sicura e con la massima conformità al GDPR

La soluzione NAS Buffalo TeraStation™, specificamente progettata per le SMB, fornisce le seguenti funzioni che garantiscono la massima conformità al GDPR.

- Non è previsto alcun accesso secondario; pertanto, gli hacker non possono accedere ai dati archiviati attraverso metodi comuni come protocolli SSH o server Telnet. In breve, i dati non possono essere soggetti ad atti di pirateria né distrutti.
- Non è prevista alcuna opzione o funzione nel sistema operativo del firmware TeraStation™ per la modifica o l'aggiunta di funzioni. Essenzialmente, il sistema è bloccato e, di conseguenza, è negata la potenziale creazione inconsapevole di vulnerabilità alla sicurezza che possano essere sfruttate dagli hacker.
- Un'opzione software consente a un utente di dare la priorità alla sicurezza dei dati rispetto all'accesso al sistema disabilitando i ripristini esterni.
- I dispositivi TeraStation™ sono fisicamente protetti da blocchi dei cavi e unità disco rigido bloccabili. Questi vincoli fisici proteggono l'hardware dal furto effettivo mentre l'autenticazione di avvio nel software nega l'accesso ai dati in qualsiasi caso.
- Include la crittografia hardware AES per le unità disco rigido. Tale crittografia non è attiva per impostazione predefinita ma può essere facilmente attivata. Essenzialmente, viene bloccata l'unità disco rigido in modo che, se l'unità viene rimossa, non sia possibile accedere ai dati.
- Include protocolli di condivisione dei file (HTTPS, SFTP) per l'accesso sicuro locale e remoto. I dati non vengono mai inviati come testo non crittografato su Internet e ciò ne impedisce la lettura da terze parti o hacker.
- Per migliorare le prestazioni, l'affidabilità e la sicurezza dell'archiviazione dei dati, le modalità RAID sono preconfigurate in fabbrica.
- Ogni TeraStation™ include la sostituzione con scambio a caldo ininterrotto delle unità disco rigido per garantire che i dati archiviati siano sempre integri.
- Il firmware TeraStation™ non può essere infetto dai virus poiché si trova all'interno di un sistema chiuso. Detto questo, i file e i file condivisi utilizzati tra computer, tablet e smartphone sono sempre a rischio di infezione malware, come ransomware, spyware e Trojan, quando tali dispositivi si connettono alla soluzione di archiviazione. L'opzione antivirus, aggiornata di frequente con le ultime impronte digitali dei virus e progettata per rilevare minacce zero-day, garantisce la sicurezza di tutti da malware.
- Le diverse opzioni di backup disponibili consentono l'archiviazione sicura dei file all'interno o all'esterno della soluzione NAS. Tali opzioni includono backup regolari, replica dei dati, failover, backup su cloud, backup su USB o NAS e backup su PC e server.

Esistono diversi modelli Buffalo TeraStation™, ciascuno progettato per soddisfare le specifiche esigenze delle organizzazioni di varie dimensioni.

Responsabile per la protezione dei dati

Per garantire la corretta conformità delle SMB al GDPR, è necessario un responsabile per la protezione dei dati che si assuma la responsabilità della gestione e della protezione dei dati del cliente.

La nomina di un responsabile per la protezione dei dati assicura un'attenzione costante.

Il responsabile per la protezione dei dati può identificare lacune, tracciare esigenze e introdurre e controllare processi di gestione che si adattano ai requisiti.

In breve, tale persona diventa l'esperto della conformità al GDPR e assume un'importanza fondamentale per il successo della conformità.

Definizioni del GDPR

Il GDPR si riferisce ai controllori dei dati, agli elaboratori dei dati e ai soggetti dei dati.

- I controllori dei dati sono le organizzazioni che raccolgono i dati dei residenti dell'Unione Europea, ad esempio, un'azienda online o offline che commercia nell'Unione Europea e gestisce le informazioni personali dei clienti come nomi, indirizzi e informazioni di pagamento.

- Gli elaboratori dei dati sono organizzazioni che elaborano i dati per conto del controllore dei dati come il provider di servizi cloud.

- Il soggetto dei dati è un cittadino o un residente dell'Unione Europea le cui informazioni sono trattate da un controllore dei dati o elaborate da un elaboratore dei dati.

Molte SMB sono sia controllori dei dati che elaboratori dei dati.

Definizione dei dati personali in base al GDPR

I dati personali sono definiti come tutte le informazioni correlate a un cittadino dell'Unione Europea che possono essere utilizzate per identificare direttamente o indirettamente la persona.

Tali informazioni includono nome, foto, un indirizzo e-mail, dettagli bancari, post su siti Web di social network, informazioni mediche e persino l'indirizzo IP di un computer.