syneto
your data • our business

SOLUTIONBRIEF

Conformità con il GDPR: cosa c'è da sapere

Cosa bisogna conoscere sul GDPR, e come prepararsi

Come la "giusta" infrastruttura IT può aiutare un' azienda ad essere conforme al GDPR

Riassunto

Il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation) sarà in vigore a partire da maggio 2018. Tutte le aziende che gestiscono dati di proprietà di cittadini europei dovranno aderirvi, indipendentemente dalla loro ubicazione.

Questo articolo espone quello che la tua organizzazione deve conoscere sul GDPR e come un'infrastruttura correttamente pensata può aiutare a mantenerne la conformità, indicando possibili soluzioni. In particolare illustra come un 'infrastruttura "iperconvergente" Syneto può contribuire a raggiungere questo obiettivo.

Punti principali

Cos'è il GDPR e perché è necessario?

Il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation, regolamento UE 2016/679) è volto a unificare e migliorare le norme sulla protezione dei dati dei cittadini UE. Il GDPR sostituisce la direttiva 95/46/EC.. Secondo il sito web ufficiale del GDPR EU (www.eugdpr.org), il regolamento è stato:

> *[...] concepito per armonizzare le leggi sulla riservatezza dei dati in tutta Europa, per proteggere ed assistere la riservatezza dei dati dei cittadini UE e per cambiare il modo in cui le organizzazioni del nostro continente gestiscono la riservatezza dei dati".*

Essendo mirato a migliorare una direttiva del 1995, esso mantiene gli stessi principi chiave in materia di protezione dei dati. L'utilizzo di dati ha fatto molta strada negli ultimi 20 anni, pertanto questo Regolamento presenta un maggiore livello di complessità, in quanto riguarda anche settori considerati di scarso interesse nel 1995. Per conformarsi al GDPR, le organizzazioni dovranno migliorare la gestione di persone e processi, monitorando il loro utilizzo dei dati.

Perché? Le innovazioni tecnologiche e la globalizzazione hanno avuto un forte impatto sul modo in cui la maggior parte delle aziende lavorano: quasi tutte le organizzazioni oggi gestiscono infatti i dati personali degli utenti. Tali dati potrebbero essere sfruttati in modi potenzialmente dannosi per gli utenti, come dimostrato dalla recente impennata degli attacchi informatici, che ha interessato non solo le piccole aziende, ma anche grandi realtà imprenditoriali come Yahoo e Uber.

Cosa sono i dati personali? Qualsiasi informazione può essere usata per identificare il soggetto interessato: nome, indirizzo e-mail, post sui social media, informazioni sanitarie, luogo di residenza, coordinate bancarie, indirizzo IP, cookie, etc

A chi si applica il GDPR? A tutti i responsabili e i titolari del trattamento dei dati, che gestiscono i dati personali di cittadini europei. Per **titolare del trattamento dei dati** si intende "*la persona fisica o giuridica, l'ente pubblico, l'agenzia o qualsiasi altro soggetto che, individualmente o congiuntamente ad altri, stabilisce le finalità e gli strumenti del trattamento di dati personali*", mentre **il responsabile del trattamento dei dati** "*gestisce il trattamento di dati personali per conto del titolare*".

Quali sono i cambiamenti di cui essere al corrente?

Sanzioni: La mancata conformità con il GDPR comporterà elevate sanzioni pecuniarie; le aziende e le organizzazioni che agiscono in violazione del GDPR potranno essere sanzionate con un'ammenda fino al 4% del fatturato annuo globale o pari a 20 milioni di €, a seconda di quale dei due importi sia superiore.

Applicabilità extraterritoriale: il GDPR si applica a tutte le aziende e le organizzazioni che gestiscono dati personali di cittadini dell'UE, indipendentemente dalla loro ubicazione. Ciò implica che, se un'azienda non avente sede nell'UE intrattiene rapporti commerciali in Europa, essa sarà comunque tenuta a conformarsi.

Privacy by design: le aziende saranno responsabili di garantire la protezione dei dati, implementando misure tecniche e organizzative adeguate; la protezione dei dati non potrà più essere considerata un compito supplementare, ma dovrà essere una funzionalità predefinita dei sistemi utilizzati dalle aziende.

Consenso: il GDPR prevede inoltre che le aziende si facciano carico di chiedere agli interessati il consenso per la gestione dei loro dati in modo chiaro e comprensibile. Agli interessati dovrà essere concessa la possibilità di revocare il proprio consenso con la stessa facilità con la quale lo hanno prestato.

Diritto di accesso e diritto all'oblio: tutte le aziende che gestiscono dati personali avranno l'obbligo di fornire agli interessati una copia dei dati e le informazioni su dove tali dati vengono memorizzati; inoltre, saranno tenute a cancellare o interrompere su richiesta la condivisione dei dati con terze parti.

Notifiche di violazione: le aziende avranno l'obbligo di informare sia i clienti sia i titolari del trattamento dei dati in caso di violazione dei dati, entro 72 ore dal momento in cui tale violazione si è verificata. La mancata osservanza di tale norma potrebbe comportare l'addebito di sanzioni elevate.

Responsabili della protezione dei dati (RPD): Le organizzazioni che gestiscono dati personali (titolari e responsabili del trattamento dei dati) saranno tenute a nominare un RPD. Tale figura potrà essere un membro dello staff, una persona assunta allo scopo o un contraente esterno.

Portabilità dei dati: Le persone interessate avranno il diritto di trasferire i propri dati da un titolare del trattamento dei dati (azienda o organizzazione) a un altro; le aziende che gestiscono i dati dovranno essere in grado di condividere i dati in un formato di uso comune.

Come può essere impattata la tua organizzazione?

La protezione dei dati è sempre stata importante, ma ora, grazie al GDPR, le aziende avranno l'obbligo legale di garantirla. La mancata osservanza può comportare conseguenze molto negative sulla conduzione degli affari dell'organizzazione:

Perdita di denaro: Le aziende e le organizzazioni che agiscono in violazione del GDPR possono essere sanzionate con un'ammenda fino al 4% del fatturato globale annuo o pari a 20 milioni di €, a seconda di quale dei due importi sia superiore. Per evitare il pagamento delle sanzioni, l'organizzazione dovrà migliorare i propri processi aziendali, tecnici e organizzativi.

Perdita della fiducia dei clienti: Le aziende sono tenute a garantire la sicurezza dei dati dei propri clienti. In caso di perdita di dati, la fiducia dei clienti nell'azienda potrebbe venire meno e questi potrebbero decidere di rivolgersi alla concorrenza. Per scongiurare tale pericolo, è necessario garantire la completa protezione dei dati.

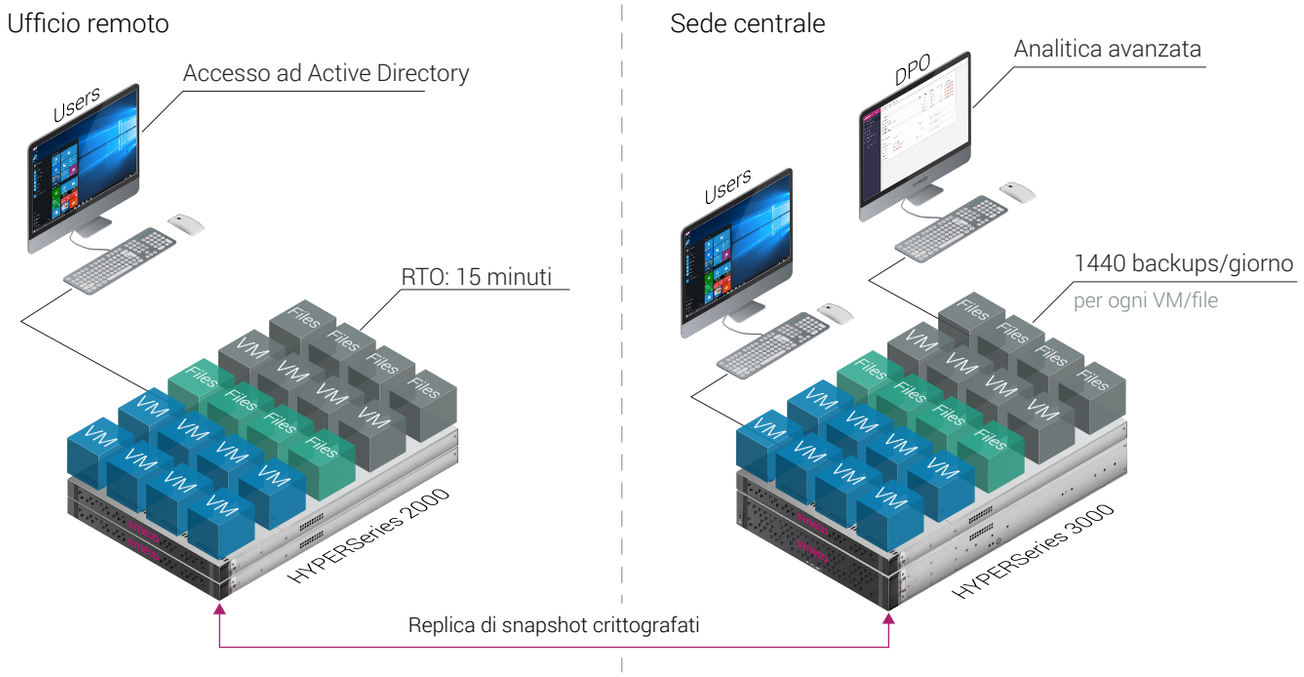
Potenziale perdita di affari: A partire da maggio 2018, le aziende che non si conformeranno al GDPR e non saranno in grado di proteggere i dati dei clienti perderanno la propria credibilità e, potenzialmente, importanti opportunità di business.

In che modo una soluzione Syneto può esserti utile per conformarti al GDPR?

Scegliere la giusta infrastruttura IT può aiutarti a superare le sfide connesse al rispetto degli standard normativi del GDPR. La soluzione Syneto si integra facilmente con tutti gli attori e i processi della tua azienda grazie a:

Una policy flessibile e granulare per tutte le applicazioni e i file dell'infrastruttura, facilmente gestibile dal RPD

Strumenti avanzati di gestione dell'utente e integrazione del server di Dominio che garantiscano che solo i dipendenti in possesso delle giuste credenziali possano accedere ai dati.



Disposizioni del GDPR

Art. 5 - Trattamento dei dati personali

(1) f) I dati personali devono essere trattati con modalità atte a garantire la sicurezza dei dati stessi, ivi compresa la protezione dal trattamento non autorizzato o illecito e dalla perdita, distruzione o danneggiamento accidentale, attraverso la messa in atto di adeguate misure tecniche o organizzative.

(2) Il titolare del trattamento (tu, in qualità di proprietario) sarà responsabile di, e dovrà essere in grado di comprovare la conformità e la responsabilità.

Art. 24 - Responsabilità del titolare del trattamento

(1) Il titolare del trattamento implementerà misure tecniche adeguate per garantire ed essere in grado di comprovare che i dati vengono gestiti in conformità con il regolamento.

(2) Le misure di cui al paragrafo 1 dovranno includere l'implementazione di adeguate policy di protezione dei dati da parte del titolare del trattamento.

Art. 32 - Sicurezza del trattamento

(1) I titolare/responsabile del trattamento implementerà misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio, ivi comprese:
b) la capacità di garantire la riservatezza, integrità, disponibilità e resilienza senza interruzioni dei sistemi e servizi di elaborazione;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di inconvenienti fisici o tecnici;

(2) Nella valutazione del livello di sicurezza adeguato, si terranno in particolare considerazione i rischi connessi alla gestione, specialmente quelli conseguenti a distruzione accidentale o illecita, perdita, modifica, diffusione non autorizzata di, o accesso non autorizzato a, dati personali trasmessi, memorizzati o altrimenti trattati.

In che modo Syneto può esserti utile

Sicurezza e ripristinabilità dei dati

Il file system di SynetoOS (gestito da tutti i prodotti Syneto) è appositamente concepito per garantire la sicurezza e la ripristinabilità dei dati. I dati personali possono essere ripristinati a seguito di attacchi di software dannosi, cancellazione accidentale o perdita fisica della piattaforma.

Grazie al sistema Syneto, sarai in grado di dimostrare facilmente il livello di protezione e la ripristinabilità di qualsiasi file o server virtuale contenenti dati personali.

I dati sono protetti dal danneggiamento

Syneto ti consente di gestire correttamente gli aspetti tecnici connessi alla protezione dei dati personali. Il tuo dispositivo Syneto è in grado di mantenere i dati al riparo da eventuali danneggiamenti e renderli recuperabili a seguito di virus, cancellazioni o disastri naturali. I dispositivi Syneto ti offrono backup automatici e policy di replica che garantiscono una protezione adeguata e dimostrabile.

Riservatezza e tempi di inattività limitati

I prodotti Syneto sono concepiti per garantire la riservatezza interfacciandosi con software di Controllo dell'accesso ai dati, come Microsoft Active Directory. I dispositivi e SynetoOS sono inoltre progettati per limitare i tempi di inattività dei sistemi di elaborazione (VM in hosting o condivisione di file) e ripristinare i sistemi in soli 15 min.

I sistemi Syneto sono dotati di funzionalità di DR integrate e di un'unità di ripristino dati dedicata che può "replicare" l'intera infrastruttura IT in soli 15 min.

I sistemi Syneto sono concepiti per prevenire la perdita di dati in qualsiasi delle circostanze indicate. I dati danneggiati vengono riparati automaticamente durante i controlli di integrità, l'accesso ai dati è controllato tramite l'integrazione con i server di Dominio e può essere ripristinato a seguito di attacchi di software dannosi, cancellazioni, guasti hardware o disastri naturali.

Contact Information
Symbol Palace, Via Cefalonia 55,
25124, Brescia, Italy
t. (+39) 030 7687 766

twitter: @syneto
youtube.com/SynetoStorage
e. sales@syneto.eu

syneto
www.syneto.eu