arcserve®

PUNTO DI VISTA

Gestione dati nel rispetto della General Data Protection Regulation (GDPR)

Di Christophe Bertrand, VP Product Marketing

Storicamente, le informazioni personali come nome, indirizzo, numero di telefono, data di nascita, sesso, età e origine etnica sono stati raccolti con il consenso dei proprietari, persone che compilavano moduli, prenotavano le vacanze, acquistavano biglietti e partecipavano all'estrazione di premi. L'evoluzione di social media, smartphone e applicazioni cloud, ha fatto sì che le informazioni personali identificabili (PII) vengano raccolte in modi molto più indiretti. Per esempio, l'indirizzo IP e il luogo dove ci si trova vengono rilevati dal telefono anche mentre si è in un bar per la pausa caffè.

Troppo spesso gli individui hanno poca o nessuna conoscenza dell'ampiezza e dei modi in cui i loro dati sono stati registrati, analizzati e condivisi. Alla fine, questa combinazione esplosiva di raccolta sempre più diffusa di dati personali e aumento di incidenti legati alla perdita di informazioni ha portato alla definizione di nuove e più severe normative.

Con la sempre più rapida diffusione della tecnologia e la natura senza confini della moderna economia digitale, i governi hanno dovuto provvedere a garantire la protezione e a migliorare i diritti fondamentali dei proprietari dei dati. Il 25 maggio 2018 diventerà legge la normativa più completa del mondo sulla privacy dei dati, la General Data Protection Regulation (GDPR) dell'Unione europea.

La GDPR dà diritto ai residenti dell'UE di verificare quali loro dati le aziende hanno registrato e di togliere il consenso all'utilizzo, ordinando in pratica la distruzione delle informazioni. Secondo l'articolo 12 della GDPR, questa richiesta deve essere gratuita, semplice da eseguire ed essere portata a termine senza "ritardo non motivato e al massimo entro un mese."

La normativa si propone di armonizzare i 28 stati dell'UE e di incoraggiare le aziende ad essere più affidabili, trasparenti e responsabili rispetto ai dati che conservano. Ogni ente che conserva o processa dati personali di residenti UE sarà tenuto a conformarsi alla nuova legislazione, indipendentemente dalla sede dell'azienda. Inoltre, ogni residente in UE avrà il diritto di controllare quali dei propri dati ogni azienda conserva.

Per l'implementazione della nuova legge la UE ha posto come scadenza maggio 2018, dato che per la maggior parte delle aziende saranno necessari tempo e investimenti per supportare i processi e le funzioni obbligatori per la GDPR. Considerato l'ambito e l'impatto trasformativo della GDPR è importante che le aziende prendano in esame il modo in cui trattano i dati personali.

Il mancato rispetto della normativa sarà punito con sanzioni il cui importo è il maggiore tra il 4% del fatturato totale e 20 milioni di euro. Nella pratica l'adeguamento è stato capovolto: invece di scegliere semplicemente di pagare la sanzione per evitare di adeguarsi alla normativa, le aziende devono investire ora per essere pronte alla GDPR o saranno soggette a multe consistenti.

La GDPR richiede riforme complete e azioni rapide e pone indicazioni precise da seguire:

- Responsabilità e Governance: mantenere la documentazione rilevante sulle attività di data processing e implementare misure che dimostrino l'aderenza alle norme, come per esempio revisioni contabili.
- Notifica delle violazioni: eventuali violazioni devono essere notificate all'autorità competente entro 72 ore dal momento in cui l'azienda ne viene a conoscenza.
- Limite di conservazione: i dati personali non possono essere conservati per un tempo più lungo di quanto necessario allo scopo per il quale erano inizialmente stati raccolti.
- Diritti individuali: un individuo può richiedere la cancellazione o la rimozione di dati personali nel caso in cui non ci sia una motivazione stringente per la loro conservazione.

Tra questi obblighi, Arcserve richiama l'attenzione sul bisogno di protezione e sulla prevenzione della perdita di dati. Le infrastrutture IT devono appoggiarsi alle tecnologie più avanzate per evitare incidenti.

Oggi, non c'è una sola soluzione che soddisfi tutti gli aspetti della GDPR. Per quanto riguarda l'IT e i processi legati ai dati ci sono diversi aspetti da tenere in considerazione, tra i quali backup e archiviazione.

Implicazioni per backup e archiviazione

L'articolo 5 della GDPR espone i principi chiave per la protezione dati e definisce come le aziende processano le informazioni personali, come possono essere conservate e come dovrebbero essere protette. L'articolo 5 afferma che le aziende possono conservare copie di backup e archivio dei dati a condizione che questi siano elaborati in modo da assicurare un'adeguata sicurezza delle informazioni personali.

L'articolo 5 della GDPR prevede che i dati personali siano:

(a) trattati in modo legittimo, equo e trasparente in relazione agli individui;

(b) raccolti con scopi specificati, espliciti e legittimi e non processati ulteriormente in modo incompatibile con questi scopi; un'ulteriore elaborazione a scopo di archiviazione nell'interesse pubblico, scientifico o di ricerca storica o statistica non deve essere incompatibile con lo scopo iniziale;

(c) adeguati, rilevanti e limitati a quanto necessario in relazione agli scopi per i quali sono processati;

(d) accurati e, quando necessario, mantenuti aggiornati; si deve provvedere a ogni passo possibile per assicurare che eventuali dati personali inaccurati, in considerazione dello scopo per il quale sono elaborati, siano cancellati o rettificati senza ritardi;

(e) mantenuti in una forma che consenta l'identificazione dei soggetti proprietari per il solo tempo necessario allo scopo per il quale i dati sono stati raccolti; le informazioni personali possono essere mantenute più a lungo solo nel caso in cui vengano elaborate esclusivamente per archiviazione nell'interesse personale, scientifico o di ricerca storica o statistica e a condizione che vengano implementate misure tecniche e organizzative appropriate, come richiesto dalla GDPR, in modo da salvaguardare i diritti e la libertà degli individui;

(f) processati in modo da assicurare appropriata sicurezza delle informazioni personali, tra cui protezione contro elaborazioni non autorizzate o non previste dalla legge e contro perdite accidentali, distruzione o danno, con l'utilizzo di tecniche o misure organizzative appropriate.

La GDPR comprende norme che promuovono responsabilità e governance. Tali norme completano i requisiti di protezione dati della GDPR. Il nuovo Principio di responsabilità contenuto nell'articolo 5(2) richiede alle aziende, attribuendo loro la responsabilità, di dimostrare il rispetto della normativa.

(a) Implementando misure tecniche e organizzative appropriate per assicurare e dimostrare il rispetto delle norme.

(b) Conservando la documentazione rilevante sulle attività di elaborazione.

(c) Dove appropriato, incaricando un addetto alla protezione dati (data protection officer).

(d) Implementando misure che rispettino i principi di protezione dati fin dalla progettazione e la protezione dati di default.

(e) Dove necessario, utilizzando valutazioni d'impatto sulla protezione dati.

Arcserve rispetta in modo unico i requisiti della GDPR

La GDPR richiede una data governance potenziata per quanto riguarda il backup e l'archiviazione. I tradizionali prodotti di backup e archiviazione puntano principalmente a risolvere i problemi di gestione delle informazioni individuali e per questo sono carenti rispetto al garantire il rispetto completo della GDPR. Arcserve ha adottato un approccio unico fornendo un robusto set di prodotti che soddisfa le esigenze più ampie dettate dai requisiti della GDPR.

Un esteso processo richiede di definire in cosa consistono i dati personali in ogni azienda. Le aree più ovvie dove si trovano comprendono database, e-mail e workstation. La definizione di informazioni personali è piuttosto ampia e include posta elettronica personale, indirizzi e-mail e altri dati che le aziende raccolgono non solo come parte delle strategie di marketing e business ma anche nell'ambito dei normali processi di backup e protezione dati. La GDPR richiede che i proprietari diano il consenso sui propri dati nel momento in cui sono raccolti. In sostanza, le copie di backup e le e-mail contengono dati personali che costituiscono una questione ulteriore: le aziende devono gestire tutte le copie di backup e le e-mail archiviate secondo le norme

della GDPR. Le copie di backup sono fatte per proteggere i dati personali offsite in caso di disastro. È piuttosto normale che le organizzazioni abbiano una dozzina o più copie di ogni backup.

Se si conservano dati di backup di abitanti dell'Unione europea, il backup deve essere nell'Unione europea ed eventuali copie di lavoro, su nastro o nel cloud dovrebbero rimanere in UE, a meno che il cliente non abbia dato il consenso alla conservazione all'esterno della UE.

Le aziende che archiviano l'e-mail devono fare molta attenzione alle norme della GDPR. È pratica comune che negli archivi di e-mail sia conservata posta di anni: per motivazioni di business, requisiti normativi e legali. Nel caso in cui l'utente tolga il consenso, l'amministratore deve avere a disposizione gli strumenti standard forniti dalla soluzione di archiviazione per identificare le e-mail e toglierle dall'archivio. I log dell'attività sono indispensabili per conservare la prova della distruzione in caso di audit.

Con l'attuale tecnologia, non c'è modo di eliminare le informazioni personali dal backup, indipendentemente dal vendor.

- Potrebbe anche presentarsi il rischio di frode in massa se non si riesce a far "sparire" facilmente un individuo da tutti i dati correnti e di archivio/backup.
- Potrebbe verificarsi anche un conflitto con le norme di compliance che sostengono la conservazione e/o l'immutabilità dei dati.

È consentito tenere le informazioni personali nel proprio backup, anche se l'individuo ha esercitato il diritto di essere cancellato. MA... non si ha il diritto di fare il restore di quei dati (a meno che non ci sia una motivazione legale, come una causa civile).

- L'adesione alla GDPR prevede che le informazioni personali conservate in copie di backup siano segnate come eliminate e non possano essere ripristinate se l'utente nega il consenso.
- Se si deve effettuare un ripristino che include dati personali che dovrebbero essere cancellati, in questo caso si devono eliminare di nuovo.
- C'è consenso sul fatto che il diritto di essere dimenticati si debba applicare più a dati attuali/di produzione che a quelli di archivio o backup.

In generale i dati, compresi i backup, devono essere protetti da violazione (per esempio con la crittografia). Le soluzioni di Arcserve hanno queste funzionalità.

Se si conservano dati che si ritengono personali o sensibili, come le informazioni sui clienti, i dati di cittadini dell'Unione europea (backup) devono risiedere nell'Unione europea (sede).

Bisogna ammettere che in questo momento nella GDPR si rilevano alcune aree grigie, sia per le aziende che per i vendor. Le interpretazioni e i precedenti aiuteranno nelle future implementazioni.

Arcserve Unified Data Protection (UDP)

Arcserve fornisce funzionalità da grande azienda senza la complessità spesso associata con le soluzioni enterprise di protezione dati. I team IT piccoli e sovraccarichi di lavoro possono salvaguardare i dati in cloud, in postazioni virtuali e fisiche proteggendoli da e per qualsiasi destinazione, configurando e gestendo tutti gli aspetti della protezione dati attraverso un'unica, semplice ed elegante console utente. Seguendo il cambiamento delle esigenze aziendali o l'evoluzione dei requisiti, i team IT possono facilmente attivare funzionalità con prestazioni elevate senza costosi e onerosi aggiornamenti o aggiunta di ulteriori soluzioni dedicate.

Uno dei principali requisiti della GDPR, come definito nell'articolo 5(2), è che "il controllore deve essere responsabile di, ed essere in grado di dimostrare, il rispetto dei principi."

Da una prospettiva di compliance, regolari test sul sistema di backup e recovery e reporting sulla protezione dati sono un buon modo per

il Data Protection Officer (nuovo ruolo) di dimostrare il rispetto della norma e l'efficace protezione/salvaguardia dei dati.

Arcserve UDP può aiutare fornendo:

- SLA e report di Assured Recovery che documentano la sicurezza dei dati, compreso quanto spesso i dati sono protetti e in quanto tempo si può ripristinare una copia di backup.
- I report standard documentano quali backup si avviano, quali dati sono protetti e dove sono conservati.
- I report di Retention Policy documentano quanto a lungo sono conservate le copie di backup e quando vengono distrutte.

Benefici di UDP

Data Protection, recovery e affidabilità potenziate

- Architettura integrata che riunisce all'interno di una sola console le tecnologie fondamentali per la protezione dati
- Soluzione ricca di funzioni che supportano un'ampia varietà di ambienti
- Piani di protezione personalizzati per risolvere particolari esigenze di protezione dati
- Reportistica avanzata per dimostrare l'adesione ai principi della GDPR

Migliorata efficienza operativa

- L'efficienza dell'amministratore è ottimizzata grazie alla console di gestione integrata di Arcserve.
- Facilità d'uso e ampie funzionalità combinate per migliorare il time to value
- Riduzione del consumo di storage e risorse di rete

Funzionalità avanzate per dimostrare l'adesione ai principi della GDPR

- La crittografia protegge le copie di backup per salvaguardare i dati secondo le norme della GDPR
- Opzioni di recovery flessibili per gestire le copie di backup della compliance alla GDPR
- Le opzioni riguardanti la retention consentono anche la conservazione a lungo termine, conservazione legale e cancellazione sicura
- Possibilità di testare, misurare e riferire i processi di recovery per la compliance alla GDPR

Arcserve UDP Archiving

Arcserve UDP Archiving consente alle aziende di rispondere con facilità alle sfide legate a ricerca di e-mail, compliance e rischio giuridico con una soluzione ad hoc che supporta

l'implementazione on-premise e su cloud privato e pubblico. I team IT piccoli e sovraccarichi di lavoro possono ottimizzare l'efficienza operativa e ridurre i costi, configurando e gestendo tutti gli aspetti della protezione dati attraverso un'unica, semplice ed elegante console utente.

Come soluzione nuova all'interno di Arcserve UDP, la tecnologia e-mail fornisce tutti gli strumenti che possono aiutare gli utenti a gestire le e-mail archiviate per rispondere ai requisiti della GDPR. Supporta un'architettura multitenant, consentendo alle aziende multinazionali e decentralizzate di separare l'archivio della posta per sede, divisione o dipartimento. Per esempio, la e-mail generata in un Paese europeo può essere gestita e conservata separatamente da quella originata in America del Nord.

Arcserve UDP Archiving è una soluzione di archiviazione per la e-mail progettata specificamente per gestire la posta elettronica secondo disposizioni come quelle della GDPR e offre diversi controlli standard per rispondere rapidamente alle richieste di eliminazione secondo la nuova normativa. La soluzione UDP Archiving può inoltre aiutare a dimostrare la cancellazione dei dati personali dagli archivi.

Quando le persone negano il loro consenso, gli amministratori possono utilizzare i tool eDiscovery integrati per trovare, identificare e cancellare rapidamente tutte le e-mail inviate o ricevute dal singolo individuo. Gli amministratori hanno accesso a log di archiviazione dettagliati che riportano tutte le azioni eseguite come prova della distruzione. Bisogna comunque fare attenzione a non creare conflitti con i requisiti di compliance. La legislazione GDPR non è necessariamente chiara a questo proposito.

Vantaggi di Arcserve UDP Archiving a colpo d'occhio

Amministrazione per archiviazione, ricerca e conservazione da un'unica console

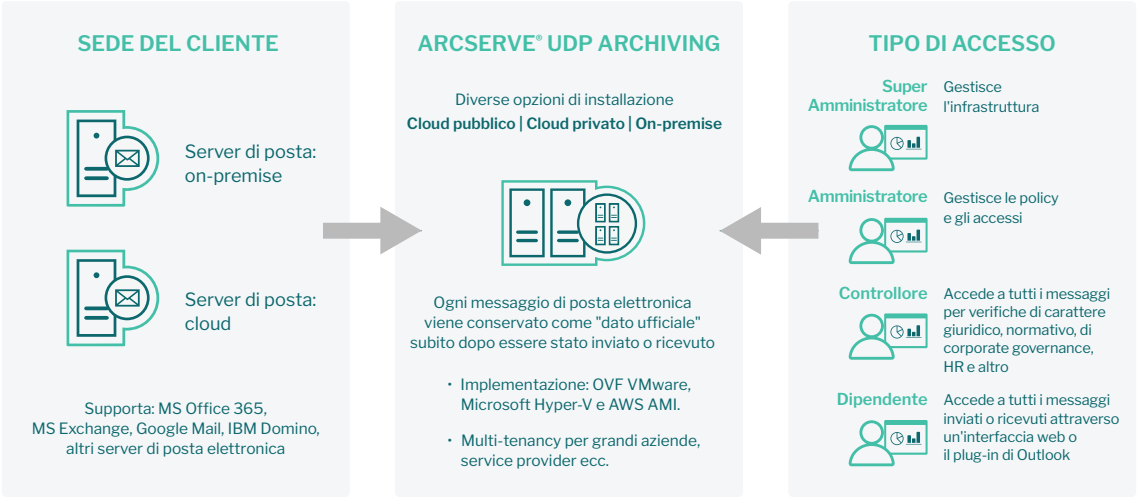
Controllo multitenant per dipartimento, divisione o sede

Ricerca e rimozione di e-mail dall'archivio in modo veloce e potente

Nessun limite alle caselle e-mail per ricerca

Report di activity log come prova della distruzione

Topologia di Arcserve UDP Archiving



Conclusione

La GDPR garantisce ai residenti UE il diritto di togliere il consenso e ordinare la distruzione delle proprie e-mail e di altre informazioni personali, aprendo la strada a un nuovo scenario di requisiti per la compliance ai quali le aziende devono aderire. Anche se il diritto di cancellare i dati personali è l'aspetto maggiormente enfatizzato, è solo uno dei tanti previsti dalla nuova normativa. Il fatto che sia chiaramente focalizzata sulla protezione dei dati personali, coinvolge anche decisioni che riguardano operazioni di backup e recovery.

I team incaricati di gestire dati di backup ed e-mail hanno bisogno di tool potenti ma anche facili da utilizzare, che consentono loro di identificare rapidamente i dati personali e di rimuoverli dai sistemi. Arcserve UDP e la sua soluzione di archiviazione garantiscono le funzionalità necessarie per dimostrare la rispondenza ai principi della GDPR, compresi backup e recovery da una console centralizzata, recupero granulare con la possibilità di escludere file e una gamma completa di funzionalità di tracking e reporting della compliance.

Nel caso in cui un utente neghi il suo consenso, l'amministratore può facilmente identificare e rimuovere le e-mail personali archiviate con strumenti standard, assicurando in questo modo la compliance alla GDPR ed evitando potenziali multe e sanzioni. Arcserve UDP e la sua soluzione di archiviazione costituiscono un tassello importante per una strategia GDPR resiliente.

Per ulteriori informazioni su Arcserve, **si prega di visitare il sito web** arcserve.com