SOLUTION BRIEF
GDPR UE

La compliance GDPR: cosa fare per adeguarsi alla nuova normativa

ca technologies

Le aziende si attengono a direttive e normative in materia di protezione dei dati da oltre due decenni; ma il Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation), una revisione della legislazione vigente in materia di protezione dei dati della Commissione europea, mira a rafforzare e a unificare queste normative per i cittadini dell'UE. Essenzialmente il GDPR vuole attribuire ai cittadini il controllo dei loro dati personali e semplificare il contesto normativo per le attività internazionali. Cosa è richiesto alle aziende già conformi alla direttiva 95/46/CE, da un punto di vista tecnologico, per adeguarsi al GDPR?

Sezione 1:

Introduzione al GDPR

Entro il 25 maggio 2018, qualsiasi azienda che elabori dati personali di cittadini dell'UE dovrà adeguarsi al GDPR. Questo regolamento introduce nuovi requisiti di protezione dei dati che interessano la maggioranza dei business in tutti i settori. Le aziende che non si adegueranno al GDPR possono essere soggette a sanzioni pecuniarie amministrative fino a 20.000.000 euro, o fino al 4% del loro fatturato globale, a seconda di quale importo sia superiore.

Il GDPR, oltre a imporre requisiti di protezione dei dati più rigorosi, si pone anche l'obiettivo di armonizzare le normative sulla privacy in tutta l'Unione europea, il che dovrebbe in qualche misura agevolare i business nell'adozione di policy e processi di protezione dei dati maggiormente standardizzati.

Nella seguente tabella sono illustrate le categorie dei diversi requisiti del GDPR ad alto livello:

Categoria	Requisiti
Diritti degli interessati	1. Gli interessati (consultare il punto 1 delle definizioni) godono dei seguenti diritti: a. Accesso ai dati. b. Rettifica, cancellazione (diritto all'oblio) e limitazione del trattamento (consultare il punto 2 delle definizioni). c. Portabilità dei dati. d. Opposizione all'utilizzo dei dati.
Responsabilizzazione	2. I soggetti che eseguono il trattamento di dati personali sono tenuti a quanto segue: a. Implementare misure tecniche e organizzative adeguate a garantire e a dimostrare che il trattamento avviene in conformità al GDPR. b. Ottenere il consenso dell'interessato per determinate attività di trattamento. c. Implementare policy e processi di protezione dei dati adeguati. d. Conservare un registro delle attività di trattamento. e. Notificare determinate violazioni dei dati personali all'autorità di controllo. f. Notificare all'interessato determinate violazioni dei dati personali. g. Designare un responsabile della protezione dei dati ove appropriato.
Protezione dei dati fin dalla progettazione e di default	3. Implementare adeguate misure tecniche e organizzative dotate delle seguenti caratteristiche: a. Progettate per implementare in modo efficace i principi della protezione dei dati, come la minimizzazione e la pseudonimizzazione, e integrare le necessarie misure di tutela del trattamento. b. Di default evitare di rendere accessibili i dati personali senza l'intervento dell'individuo a un numero indefinito di soggetti.
Segnalazione delle violazioni dei dati	4. In caso di violazione di dati personali (consultare il punto 7 delle definizioni): a. I titolari del trattamento dei dati devono informare l'autorità di controllo entro 72 ore dal momento in cui vengano a conoscenza della violazione. b. I responsabili del trattamento dei dati (8) devono informare il titolare senza indugio dopo essere venuti a conoscenza di una violazione. c. Comunicare la violazione dei dati all'interessato (si applicano eccezioni).

Categoria	Requisiti
Anonimizzazione e pseudonimizzazione	5. Le tecniche di anonimizzazione e pseudonimizzazione dovranno essere applicate: a. Come parte dei principi di "protezione dei dati fin dalla progettazione e di default" nel trattamento dei dati personali. b. Ai dati archiviati con finalità di interesse pubblico, ricerca scientifica o storica o di tipo statistico.
Trasferimenti di dati transfrontalieri e norme vincolanti d'impresa	6. I dati personali sono soggetti a limitazioni di trasferimento: a. In paesi al di fuori dello Spazio economico europeo. b. Che non siano indicati come "adeguati" Norme vincolanti d'impresa (BCR) (9) e clausole contrattuali standard (o clausole modello) pubblicate dalla Commissione europea rimangono strumenti validi per adeguarsi alle limitazioni di trasferimento dei dati nell'UE (consultare il punto 10 delle definizioni). c. Regime dello scudo per la privacy (consultare il punto 11 delle definizioni).
Certificazioni, codici di condotta e sigilli	7. Le aziende saranno in grado di aderire a meccanismi di certificazione al fine di dimostrare esistenza e compliance con talune misure di tutela.

Definizioni estratte dal GDPR

1. **Interessato.** Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
2. **Limitazione del trattamento.** Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
3. **Titolare del trattamento.** La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
4. **Autorità di controllo.** L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.
5. **Responsabile della protezione dei dati.** Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. **Pseudonimizzazione.** Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
7. **Violazione dei dati personali.** La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

8. **Responsabile del trattamento.** La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

9. **Norme vincolanti d'impresa.** Le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

Definizioni aggiuntive rilevanti per il GDPR

10. **Paesi adeguati.** La trasmissione dei dati personali può avvenire dai 28 paesi dell'UE e da tre paesi del SEE (Norvegia, Liechtenstein e Islanda) verso un paese terzo senza necessità di ulteriori tutele.

    La Commissione ha finora riconosciuto **Andorra, Argentina, Canada** (organizzazioni commerciali), **Isole Faeroe, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera e Uruguay** come paesi in cui viene fornita un'adeguata tutela. (consultare http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

11. Per il trasferimento dei dati personali dall'UE verso gli Stati Uniti, sono disponibili vari strumenti quali clausole contrattuali, norme vincolanti d'impresa e il regime dello scudo per la privacy. Se si utilizza il regime dello scudo per la privacy, le aziende statunitensi devono anzitutto iscriversi al regime presso il Ministero del commercio americano. Gli obblighi previsti per le società ai sensi del regime dello scudo per la privacy sono inclusi nei "Principi di riservatezza". Il Ministero è responsabile della gestione e dell'amministrazione del regime dello scudo per la privacy e di garantire che le società rispettino gli impegni assunti. Per potersi certificare, le società devono disporre di una policy in materia di riservatezza dei dati in linea con i "Principi di riservatezza". Sono tenute a rinnovare la propria "autocertificazione" al regime dello scudo per la privacy su base annuale; in mancanza, non avranno più facoltà di ricevere e utilizzare i dati personali provenienti dall'UE ai sensi del regime. Un elenco di società che hanno eseguito l'autocertificazione in relazione al regime dello scudo per la privacy è reperibile sul sito del Ministero del commercio (https://www.privacyshield.gov/welcome). È inoltre disponibile un elenco delle società non più certificate ai sensi del medesimo regime.

Sezione 2:

Requisiti

Diritti degli interessati

È uno degli ambiti più importanti del regolamento. Il rigore della normativa è stato incrementato, includendo nuovi diritti che influenzeranno profondamente le modalità del trattamento e del controllo dei dati personali da parte dell'IT. È importante comprendere che il GDPR sostituisce la **Direttiva sulla protezione dei dati** (direttiva 95/46/CE) con l'obiettivo di rafforzare e unificare la protezione dei dati per gli individui all'interno dell'UE.

Mentre i diritti tradizionali di accesso (art. 15), rettifica (art. 16), cancellazione (art. 17) e opposizione (art. 21) rimangono essenzialmente invariati, è stato incluso un nuovo diritto: il diritto alla portabilità dei dati (art. 20), nonché alcune modifiche al diritto di cancellazione, includendo il concetto di diritto all'oblio (art. 17) e il diritto alla limitazione (art. 18). Questi diritti sono intesi come fondamentali e universali in tutta l'UE laddove, ai sensi della direttiva precedente, ogni Stato membro era autorizzato a interpretarli diversamente, rendendo più difficoltoso farli valere agli interessati.

Per le aziende le sfide sono molteplici e alcuni dei nuovi diritti, come la portabilità dei dati, che prevede per gli individui la facoltà di ottenere e riutilizzare i propri dati personali per i propri scopi all'interno di servizi diversi, potrebbe essere uno dei più importanti. Da qui la necessità di adottare un modello che aiuti le società a soddisfare le esigenze attuali e future.

Quando è necessario creare applicazioni aggiornate che includono dati personali compatibili con questa nuova normativa, evitando contemporaneamente il costo connesso alla modifica delle applicazioni esistenti, la risposta può essere una sola: le API.

L'adozione di un modello basato su API per l'accesso ai dati costituisce il fondamento di un'architettura a prova di futuro, che consenta all'azienda di abbracciare questa normativa e quelle future, anche grazie al fatto che le API possono essere protette, controllate e migliorate mediante l'implementazione di adeguate soluzioni software.

È stato inoltre rafforzato il requisito di ottenimento del consenso da parte dell'interessato, per cui le aziende dovranno gestire diversamente i propri rapporti con questo soggetto. Le identità digitali e la loro gestione, la governance e il controllo degli accessi giocheranno un ruolo importante per i soggetti che desiderano attenersi alla normativa.

Per quanto riguarda la compliance con il GDPR, le aziende dovranno adottare nuovi canali per comunicare con gli interessati al fine di garantire che possano esercitare correttamente i loro diritti fondamentali: ciò significa che dovranno essere applicate misure tecniche per consentire l'accesso sicuro e adeguato da parte degli individui ai loro dati. Saranno inoltre creati nuovi canali per consentire la portabilità dei dati, in modo che gli interessati possano esercitare il relativo diritto e avviare il processo di trasferimento dei propri dati al terzo designato. È pertanto fondamentale implementare controlli di accesso validi e controlli di sicurezza appropriati per questi nuovi gateway di dati.

È un'operazione che potrebbe sembrare semplice: ma i dati personali possono essere accessibili su più file system e server, ed è quindi necessario applicare correttamente la rilevazione, l'analisi e la classificazione alle infrastrutture IT prima anche solo di applicare le policy di protezione dei dati.

Responsabilizzazione

I requisiti tecnici sono integrati in tutta la normativa, ma tutto si riduce essenzialmente alla "responsabilizzazione" del titolare e/o del responsabile del trattamento dei dati. In altre parole, quando si verifica un incidente (come è quasi inevitabile che accada) il legislatore cercherà la prova che l'impresa interessata abbia adottato controlli organizzativi e tecnici adeguati per garantire il corretto trattamento dei dati personali a sensi della normativa. Le aziende devono dimostrare di aver implementato i controlli e le misure IT richiesti dalla normativa e devono monitorare e segnalare continuamente tutte le azioni intraprese. La mancata dimostrazione avrà un notevole impatto sulla determinazione delle eventuali sanzioni pecuniarie amministrative, come è espresso chiaramente nell'articolo 83.

Nell'attuale contesto IT ibrido, non è sempre facile determinare l'appartenenza dei dati presenti all'interno dei sistemi. Questo potrebbe risultare problematico per le aziende, che dovranno analizzare e individuare i dati personali nell'intero contesto delle piattaforme esistenti. In aggiunta, sarà necessario implementare soluzioni che facilitino non solo l'identificazione delle informazioni, ma anche il controllo e il monitoraggio dell'utilizzo di questi dati personali in tutto il loro ciclo di vita. In caso di incidenti, la mancata implementazione di controlli tecnici adeguati in questi ambiti sicuramente non favorirà l'azienda agli occhi del legislatore.

Protezione dei dati per default e fin dalla progettazione

L'articolo 25, considerando 2, prevede che "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". Inoltre, l'articolo 30 prevede l'obbligo di conservare un registro delle attività di trattamento.

E l'articolo 32, "Sicurezza del trattamento", al punto (b), impone "... la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento". Il punto d) prevede l'esistenza di "...una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Si tratta di un ambito molto ampio, che richiederà un approccio olistico dei processi di sviluppo del software, inclusi test, Q&A e release di nuove versioni. Tutti questi contesti IT richiederanno un livello integrato di controlli di sicurezza per garantire che i dati siano accessibili solo dai soggetti autorizzati e per le finalità specifiche per cui sono stati raccolti.

Segnalazione delle violazioni dei dati

Per diretta derivazione dal principio di responsabilizzazione già citato, i titolari e i responsabili del trattamento dei dati sono tenuti a segnalare alcune violazioni relative ai dati personali. I tipi di violazioni che richiedono la segnalazione sono descritti negli articoli 33 e 34.

L'articolo 33 prevede l'obbligo di segnalare le violazioni dei dati all'autorità di controllo competente, mentre l'articolo 34 prevede il medesimo obbligo nei confronti dell'interessato. È importante notare che, ai sensi dell'articolo 34.3, le aziende sono esentate dall'obbligo di comunicare l'incidente all'interessato se:

- il titolare del trattamento ha **messo in atto le misure tecniche e organizzative adeguate di protezione** e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura.
- Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1.

Il responsabile del trattamento comunica la violazione al titolare del trattamento senza ingiustificato ritardo; la medesima comunicazione deve avvenire da parte del titolare del trattamento all'autorità di controllo non oltre 72 ore dalla venuta a conoscenza della violazione. La segnalazione deve indicare chi ha fatto cosa e quando, nonché le azioni e le misure adottate per attenuare eventuali effetti negativi.

Anonimizzazione e pseudonimizzazione

Il GDPR introduce nuovi concetti relativi ai principi da applicare in caso di gestione e di trattamento di dati personali. La protezione dei dati personali e la riattribuzione all'interessato del controllo su di essi è l'obiettivo principale della normativa, da cui la menzione di alcune tecniche di protezione dei dati personali.

Nel capitolo II ("Principi") possiamo vedere che si intende rafforzare il modo in cui i dati personali vengono trattati ("minimizzazione dei dati") e mantenuti in una forma che limiti l'identificazione dell'interessato al minimo necessario dal punto di vista temporale. Inoltre, il trattamento dei dati personali deve avvenire in modo da garantire una sicurezza adeguata, inclusa la protezione contro il trattamento non autorizzato o illecito e contro la perdita accidentale, la distruzione o il danneggiamento, mediante l'impiego di adeguate misure tecniche e organizzative ("integrità e riservatezza").

Trasferimenti transfrontalieri di dati e norme d'impresa vincolanti

Come nella direttiva, l'articolo 45 del regolamento limita i trasferimenti internazionali di dati personali verso paesi "non adeguati" al di fuori dell'UE. L'articolo 46, considerando 2, determina le garanzie adeguate che devono essere applicate per il trasferimento di dati senza specifica autorizzazione da parte di un'autorità di controllo.

Le norme vincolanti d'impresa (BCR) (art. 47) e le clausole contrattuali standard (o clausole modello) pubblicate dalla Commissione europea rimangono strumenti validi per adeguarsi alle limitazioni di trasferimento dei dati nell'UE. L'utilizzo di questi meccanismi di trasferimento per scopi intra-gruppo dovrebbe risultare facilitato, dato che alcuni dei requisiti di autorizzazione esistenti sono stati rimossi. Verificare i punti 10 e 11 delle definizioni per quanto riguarda le implicazioni del regime dello scudo per la privacy USA.

Controllare chi ha accesso ai dati è fondamentale per soddisfare questo requisito. Le aziende dovranno condurre campagne periodiche di certificazione dell'accesso per confermare che i diritti di accesso per i propri utenti siano corretti in ogni momento. Per garantire la compliance, il responsabile della protezione dei dati (DPO) designato necessiterà di funzioni di reporting avanzate nei diversi ambiti della sicurezza IT.

In aggiunta, sarà necessario impiegare funzioni per limitare l'invio di documentazione contenente dati personali all'esterno dell'azienda, allo scopo di garantire che file contrassegnati come correlati al GDPR non vengano inavvertitamente inviati a terzi non autorizzati.

Certificazioni, codici di condotta e sigilli

Le aziende avranno facoltà di aderire a meccanismi di certificazione al fine di dimostrare l'esistenza di misure di tutela adeguate. L'articolo 42 prevede infatti un invito agli Stati membri, alle autorità di controllo e ad altre istituzioni dell'UE a istituire meccanismi di certificazione della protezione dei dati, sigilli e marchi di protezione dei dati, allo scopo di dimostrare l'osservanza della normativa. L'articolo 42 indica altresì un futuro regime di certificazione comune, il "Sigillo europeo per la protezione dei dati", che garantisca "una certificazione comune" in tutta l'UE, incrementando così coerenza e comprensione per i cittadini.

Sezione 3:

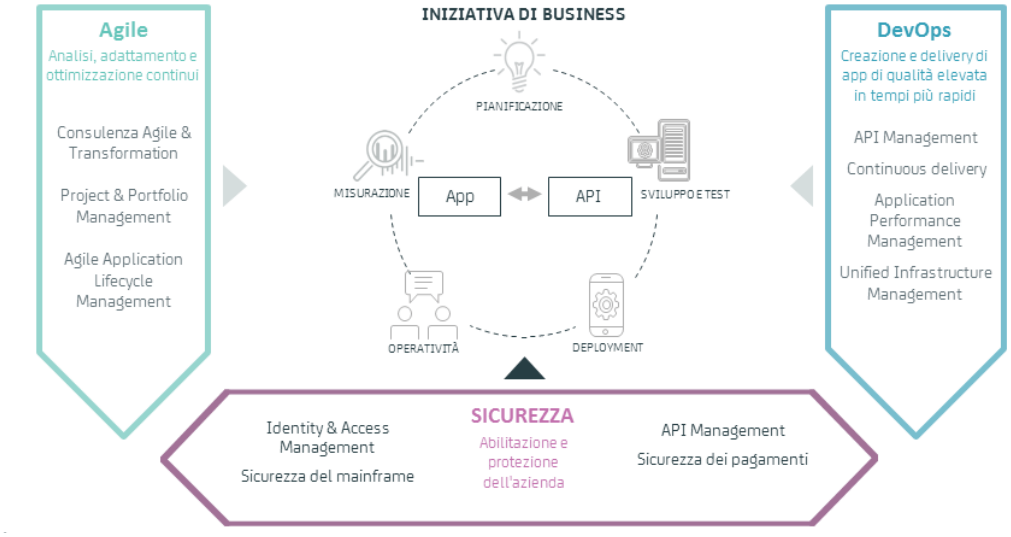
Benefici potenziali derivanti da CA Technologies

L'adesione alla normativa richiederà un approccio rigoroso, che renderà necessario il supporto dei dipartimenti Legale e IT e, in alcuni casi, di società di consulenza, per condurre valutazioni approfondite e analisi della normativa, nonché dei processi aziendali. In qualità di società software innovativa e leader nell'application economy, CA Technologies funge da guida alle aziende all'interno del processo di digital transformation e può fornire un ampio insieme di soluzioni software per aiutarle a gestire il proprio percorso di compliance.

CA Technologies fornisce alle aziende tecnologiche l'assistenza di cui hanno bisogno per essere compliant con il GDPR e a implementare i controlli previsti dal regolamento allo scopo di adeguarsi alla filosofia "sicurezza fin dalla progettazione" prevista dalla normativa medesima.

A distinguere CA Technologies dai provider di tecnologie puntuali e specifiche è il fatto che le nostre soluzioni di prodotto esauriscono praticamente ogni ambito del ciclo di vita dei dati aziendali. La combinazione delle soluzioni CA Technologies per la protezione dell'accesso ai dati, la gestione e il controllo dell'accesso degli utenti e per impedire l'accesso non autorizzato a dati personali da parte di soggetti interni ed esterni, può essere adottata dalle aziende per assicurare il rispetto della nuova normativa e la tutela dei diritti degli interessati. CA Technologies dispone degli strumenti e delle competenze per guidare le aziende attraverso l'intero processo.

CA Technologies offre una strategia DevOps completa e sicura, che non solo aumenta la velocità di sviluppo e di delivery delle applicazioni, ma garantisce anche la sicurezza delle app e dell'intero ciclo di vita del software. Le nostre soluzioni per la sicurezza includono API Management, sicurezza mainframe e i vari componenti della nostra ampia suite di sicurezza IAM. Per ulteriori informazioni sulle soluzioni di sicurezza IAM, visita ca.com/iam.



CA Technologies sulla classificazione e la localizzazione dei dati

Anche se l'azienda potrebbe essere convinta di sapere dove vengono memorizzati e controllati i dati personali, la realtà è che questi sono diffusi in tutta l'azienda, sono utilizzati e trasformati in modo ampio, e sono accessibili in modi diversi da persone diverse; ecco perché i controlli basati su applicazioni non sono sufficienti per rispettare la normativa.

Inoltre, la direttiva precedente era più focalizzata sulla protezione dei file contenenti dati personali e sulla memorizzazione delle informazioni, mentre il nuovo regolamento si concentra sul trattamento dei dati. Una conseguenza diretta della nuova era digitale, in cui i dati vengono trasformati, aggiunti, arricchiti ed elaborati a velocità elevatissime. Grazie alle moderne funzioni di analisi Big data, singole informazioni apparentemente non correlate tra loro possono essere combinate e formare dati personali, che diventano soggetti alla normativa.

Ecco perché è estremamente importante adottare un approccio di tutela sofisticato alla protezione dei dati personali, che consente di applicare livelli di controllo diversificati.

Partiamo dall'identificazione e dalla classificazione dei dati, così come dalla comprensione della posizione dei dati personali all'interno della nostra infrastruttura. Se i dati personali circolano al di fuori dei canali e dei flussi assegnati, è importante capirlo e valutare i rischi collegati.

Comprendere dove sono presenti i dati personali e chi all'interno dell'azienda ha accesso a essi è uno dei principi fondamentali del GDPR.

CA Data Content Discovery

Nell'application economy, il mainframe è sempre più connesso al resto del data center, più disponibile anche a utenti casuali, nonché soggetto alla normativa in materia di protezione dei dati. Alcuni set di dati vengono copiati dalla produzione a scopo di sviluppo o test, e quindi abbandonati; altri set rimangono orfani quando i rispettivi titolari lasciano l'azienda. Inoltre, l'iniezione avviata dagli utenti di dati non strutturati tramite UNIX® System Services può determinare la presenza di grandi volumi di dati, regolari o sensibili, nascosti all'interno del mainframe, che rappresentano per l'azienda, in caso sfuggano al controllo, un potenziale di danni monetari e alla reputazione.

Il mainframe ospita ancora oltre il 70% dei dati mission-critical. Se si utilizza una carta di debito, si prenota un volo aereo o si fa una telefonata, probabilmente si è entrati in contatto con un mainframe. Tuttavia l'application economy ha generato nuovi rischi per il mainframe, che è interconnesso a quasi tutte le applicazioni, con conseguenti violazioni dei dati spesso alla ribalta delle cronache. Per un'azienda la compromissione del mainframe e dei suoi dati, regolamentati o sensibili, sarebbe una catastrofe.

Nell'attuale contesto IT ibrido, non è sempre facile determinare quali dati presenti all'interno dei sistemi appartengono all'insieme interessato dalla normativa. Per farlo in modo corretto e sistematico, **CA Data Content Discovery** individua, classifica e protegge i dati mainframe sensibili allo scopo di gestire l'intero spettro delle piattaforme esistenti. La soluzione include policy predefinite in materia di dati personali per facilitare non solo l'identificazione delle informazioni, ma anche il controllo e il monitoraggio del loro utilizzo, come previsto in vari articoli della normativa. L'analisi avviene al 100% sulla piattaforma mainframe, evitando che i dati siano duplicati off-platform per l'analisi. In questo modo le aziende possono identificare e proteggere rapidamente i dati prima che si verifichi una violazione.

CA Identity Suite

L'articolo 25, considerando 2, prevede che "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". Inoltre, l'articolo 30 prevede l'obbligo di conservare un registro delle attività di trattamento. Ciò significa che è necessario implementare una soluzione che gestisca e disciplini il corretto accesso dei dipendenti ai dati personali, per ridurre l'esposizione inutile di tali dati.

CA Identity Suite facilita gestione e governance dell'accesso degli utenti alle applicazioni di business e ai dati sottostanti. La soluzione supporta la compliance totale con questo requisito perché fornisce report su chi ha accesso a cosa, e può condurre e gestire campagne di certificazione degli accessi per consentire all'azienda una compliance continuativa.

Un approccio comune alla compliance è la verifica periodica dell'adeguatezza dell'accesso degli utenti alle risorse aziendali. Durante la certificazione dell'accesso, i manager devono in genere esaminare gli elenchi dei privilegi dei loro subordinati diretti, per confermare o meno la necessità del relativo accesso.

CA Identity Suite rende questo processo semplice e intuitivo, incrementando così la soddisfazione degli utenti e la produttività. Adattare un processo di certificazione alle esigenze specifiche di un'azienda è fondamentale per convalidare efficacemente l'accesso e favorire la partecipazione al processo. CA Identity Suite può agevolare la revisione da varie prospettive, ad esempio dei manager degli utenti, dei titolari delle risorse o dei tecnici dei ruoli.

I processi di certificazione, o campagne, possono avvenire da ciascuna di queste prospettive, utilizzando pianificazioni, workflow e responsabili delle approvazioni diversi. Inoltre, è possibile eseguire contemporaneamente campagne multiple, ognuna focalizzata su determinati ambiti dell'azienda (ad esempio, gli utenti di una specifica business unit), o mettendo in evidenza tipi diversi di accesso (ad esempio, solo le attribuzioni sospette o l'accesso acquisito al di fuori del modello di ruoli). CA Identity Suite include controlli amministrativi e workflow per contribuire a garantire che le campagne si svolgano in base ai requisiti. Questi includono notifiche e-mail, promemoria e processi di escalation per richiedere l'approvazione a manager di livello superiore. Inoltre, quando vengono individuate discrepanze e sono necessarie modifiche ai diritti di accesso, i processi di correzione possono essere attivati tramite assegnazione di ticket ai titolari corretti, o attraverso l'integrazione con CA Identity Manager.

La normativa prevede un soggetto chiave, il DPO, che deve essere designato dall'azienda. Per questa figura saranno cruciali soluzioni tecnologiche che supportino e dimostrino tutti i controlli di sicurezza messi in atto dall'azienda per proteggere i dati personali. Le capacità di reporting delle soluzioni CA Technologies aiuteranno il DPO a dimostrare in che modo l'azienda sta rispettando la normativa, e saranno rilevanti per la creazione delle valutazioni d'impatto sulla protezione dei dati di cui all'art. 35.

CA Identity Suite include inoltre analisi integrata dei processi di identità, che fornisce informazioni dettagliate di facile elaborazione, per evidenziare il funzionamento dei processi identitari fondamentali (come l'onboarding degli utenti). Queste analisi aiutano a identificare e risolvere i colli di bottiglia e contribuiscono a garantire il rispetto degli impegni assunti a livello di SLA. CA Identity Governance include un ampio insieme di report e dashboard out-of-the-box, e supporta query ad hoc per esigenze forensi. Nei report il livello di informazioni di business e tecniche fornite varia al fine di rispondere alle esigenze dei diversi tipi di utenti. Sono inclusi, ad esempio, report separati per manager di business, tecnici dei ruoli, responsabili della compliance, revisori e personale IT.

CA Test Data Management

La normativa è destinata ad avere implicazioni importanti sul tipo di dati che possono essere utilizzati in ambienti non di produzione. Le aziende dovranno comprendere esattamente di quali dati dispongono e chi li utilizza, ed essere in grado di limitarne l'impiego alle attività per le quali è stato fornito il consenso. Un modo per evitare di esporre i dati personali agli ambienti di test consiste nell'evitarne il provisioning, anche se dei dati sia stato eseguito il masking. La generazione di dati sintetici costituisce una tecnica che potrebbe consentire alle aziende di passare ad ambienti di test completamente virtualizzati.

Durante il test e lo sviluppo di software, i dati possono finire per diffondersi tra gli ambienti di test e sviluppo e in ambienti complessi. I tester potrebbero copiare i dati nel proprio ambiente per un determinato utilizzo; ma le aziende devono sapere per quanto tempo i dati vengono utilizzati, e confermare che sono impiegati con l'autorizzazione corretta e per un scopo legittimo. La profilazione dei dati eseguita da **CA Test Data Manager** può aiutare con questo elemento chiave della compliance, individuando esattamente dove vengono archiviati dati sensibili a livello aziendale, e utilizzando l'analisi statistica per individuare i dati personali memorizzati in più formati di file e applicazioni. Utilizzando una vista cubica per generare un'immagine precisa dei dati, CA Test Data Manager identifica le informazioni sensibili riflesse nei sistemi, nei componenti o nelle applicazioni correlate. Filtri matematici e personalizzati consentono di filtrare i dati a un livello granulare, per identificare ogni istanza delle informazioni relative a un soggetto. Questi dati possono includere numeri di carta di credito, indirizzi e-mail, indirizzi di casa e simili, aiutando le aziende a realizzare il diritto alla portabilità dei dati. L'individuazione dei dati fornita da CA Test Data Manager è totalmente verificabile, affinché le aziende possano dimostrare l'applicazione dei controlli adottati a scopo di compliance.

CA API Management

Quando è necessario creare applicazioni aggiornate che includono dati personali compatibili con questa nuova normativa, evitando contemporaneamente il costo connesso alla modifica delle applicazioni esistenti, la risposta è una sola: le API.

La suite **CA API Management** consente alle imprese di affrontare le sfide connesse alla condivisione delle informazioni nell'application economy, all'insegna della massima semplicità. La soluzione combina funzionalità avanzate per l'integrazione back-end, l'ottimizzazione mobile, l'orchestrazione cloud e la gestione degli sviluppatori, nonché una capacità unica di gestire la gamma completa di questi requisiti di API Management enterprise. Utilizzando CA API Management, le aziende possono contribuire a dimostrare la compliance con la normativa senza necessità di modificare le applicazioni esistenti. Inoltre, **CA Live API Creator** può essere utilizzato per creare nuove API che includeranno i controlli appropriati ed esporranno le informazioni necessarie a terzi.

Ad esempio, utilizzando le soluzioni CA API Management, è possibile evitare di modificare le applicazioni, un'attività rischiosa e costosa, e diventa possibile controllare i comportamenti da una soluzione basata su policy e regole. In questo modo l'azienda può integrare regole per la raccolta del consenso e comunicare agli utenti le informazioni richieste dagli articoli 15 e 20 documentando, tramite **CA API Developer Portal**, le modalità possibili di accesso ai dati. Questi controlli di accesso di sicurezza sono forniti da **CA API Gateway**.

Per comprendere i vantaggi di questo approccio, è possibile calcolare il costo della modifica di tutte le applicazioni che attualmente gestiscono i dati personali all'interno dell'azienda, rispetto al costo collegato alla disponibilità di un'interfaccia singola e standardizzata, utilizzabile anche per adeguarsi ad altre normative di settore.

CA Privileged Access Manager

Gli account utente con privilegi, ottenuti in modo fraudolento o utilizzati in modo inappropriato da un utente legittimo, rappresentano il comune denominatore della maggioranza delle violazioni dei dati. Alla sempre maggiore complessità dell'ambiente corrisponde quella della difesa da attacchi sempre più sofisticati e dannosi. Il privileged access management di CA Technologies offre una soluzione completa che fornisce controlli basati su rete e su host per il cloud enterprise e ibrido.

Le aziende potrebbero pensare che sia sufficiente la protezione dell'accesso ai dati attraverso controlli di accesso basati su applicazioni; ma, nella realtà, la maggior parte delle violazioni dei dati si verificano approfittando di account utente con privilegi, e quindi bypassando i controlli di accesso, e vanificandoli. È per questo che è necessario implementare controlli di sicurezza per gestire e disciplinare l'accesso con privilegi.

CA Privileged Access Manager (CA PAM) è una soluzione automatizzata e di semplice distribuzione per il Privileged Access Management in ambienti fisici, virtuali e cloud. Disponibile come appliance hardware in hardening montabile a rack, come appliance virtuale in formato OVA (Open Virtualization Appliance) o come istanza AMI (Amazon Machine Instance), CA PAM migliora la sicurezza tutelando le credenziali amministrative sensibili, come password di root e amministratore, controllando l'accesso degli utenti con privilegi, applicando proattivamente le policy, oltre che monitorando e registrando le attività degli account con privilegi in tutte le risorse IT.

Un componente di CA PAM, **CA Privileged Access Manager Server Control** fornisce protezione completa per i server mission-critical con controlli potenti e granulari sull'accesso a livello di sistema operativo e sulle azioni degli utenti con privilegi. Dotata della capacità di implementare controlli di accesso su account superutente avanzati nativi, come root UNIX e Linux® e amministratore su Microsoft® Windows®, questa soluzione, a livello di sistema e basata su host, controlla e monitora le attività degli utenti con privilegi, migliorando la sicurezza e semplificando l'audit e la compliance.

La combinazione tra CA Privileged Access Manager Server Control per l'hardening dei server e CA Privileged Access Management fornisce all'azienda la soluzione più completa per la gestione degli utenti con privilegi e degli accessi.

CA Single Sign-On

L'application economy ha cambiato il modo in cui le aziende interagiscono con la clientela. Gli utenti richiedono accesso sempre e ovunque ai servizi online e si aspettano la stessa user experience coerente e fluida su più device e canali di accesso. In relazione al GDPR, le aziende devono trovare un equilibrio tra facilità di accesso e dati accessibili. Come fare per assicurare che solo le persone giuste accedano a contenuti sensibili e solo quando è lecito? Ad esempio, un cittadino dell'Unione europea ha il diritto di visualizzare i propri dati personali; tuttavia, potrà accedere e visualizzare i propri dati se esegue l'accesso da un paese al di fuori degli Stati Uniti? E i dipendenti dell'azienda? Magari possono accedere a questi stessi dati quando accedono dagli Stati Uniti, ma non quando si trovano in un paese al di fuori degli Stati Uniti.

CA Single Sign-On è in grado di gestire queste problematiche consentendo a dipendenti, clienti, partner e fornitori di proteggere le singole applicazioni online, a prescindere da dove vengono distribuite, dal tipo di device utilizzato per l'accesso o dalla modalità di autenticazione dell'utente al sito, diretta, tramite social media o tramite federazioni da un sito partner. Inoltre, la soluzione rafforza la sicurezza fornendo un livello di policy comune che riduce la possibilità di carenze nelle policy di accesso.

Il GDPR richiede alle aziende di concedere l'accesso agli utenti, ma di limitare il numero di persone in grado di accedere ai dati personali. Una soluzione completa per la gestione dell'accesso come CA Single Sign-On può fornire i controlli di accesso web adeguati per entrambi i tipi di utenti, da una posizione centralizzata. L'esternalizzazione di questa funzione di sicurezza dall'interno delle applicazioni supporta il principio di "sicurezza fin dalla progettazione" all'interno di DevSecOps.

CA Directory

Il GDPR introduce un'importante revisione della legislazione vigente in materia di protezione dei dati e, anche se nelle grandi imprese la maggior parte di questi dati esisteranno su mainframe, una notevole quantità di essi risiederà anche all'interno di directory. Le aziende dipendono sempre più dalle proprie applicazioni online e mobile per fornire servizi fondamentali agli utenti, e devono affrontare le sfide di performance e di disponibilità generate dai problemi dell'infrastruttura di directory sottostante, tra le quali:

- **Crescita esplosiva.** L'esplosione delle identità utente, dei device e della capacità di conservare la reattività necessaria a una user experience di livello superiore pone sfide impegnative per molti repository legacy.
- **Silos di identità.** Le varie directory distribuite da diverse unità di business nel corso del tempo oggi causano problemi tra i quali, ad esempio, una user experience scarsa, rischi per la sicurezza e maggiori costi operativi.
- **Nuovi requisiti.** I requisiti di sicurezza stanno evolvendo dalla semplice autenticazione degli utenti al monitoraggio di credenziali dettagliate e di informazioni personalizzate associate a operations di business dinamiche.

Di conseguenza, molti clienti stanno cercando di elevare l'infrastruttura di Identity and Access Management, migrando a un servizio di directory di nuova generazione che offra performance migliori con un TCO inferiore. Ma il GDPR aggiunge un ulteriore interessante sviluppo ai loro criteri di valutazione. Il servizio di directory di nuova generazione dovrebbe supportare la possibilità di suddividere la struttura delle directory su più server, consentendo all'azienda di sapere dove sono memorizzati fisicamente i dati personali. Inoltre, dovrebbe inoltre consentire di determinare selettivamente quali dati vengono replicati su diversi nodi, per evitare che lascino un'area geografica specifica.

CA Cleanup

CA Cleanup consente di identificare gli account non utilizzati per un dato periodo di tempo, nonché di generare comandi per rimuovere ID, diritti, autorizzazioni, profili e connessioni di gruppo di cui un utente dispone ma che non utilizza. Questo consente di risolvere con efficacia il problema dell'accumulo nel tempo di diritti di accesso obsoleti ed eccessivi: un requisito fondamentale per la compliance rispetto a molte normative. CA Cleanup, la cui completa distribuzione richiede solo un giorno, offre le seguenti funzionalità:

- Identificazione e rimozione di singoli utenti, diritti e gruppi di accesso non più utilizzati.
- Identificazione dei diritti (quali autorizzazioni e regole) effettivamente utilizzati e creazione di comandi per rimuovere quelli inutilizzati. Sono incluse le risorse definite dagli utenti.
- Identificazione degli ID utente effettivamente utilizzati e creazione di comandi di eliminazione per quelli inutilizzati; questo in base all'utilizzo effettivo delle funzioni di sicurezza, non alle date di "ultimo utilizzo" che risultano nel sistema, spesso inaffidabili.
- Generazione di report che descrivono diritti utilizzati e non.
- Generazione di comandi per attivare o ripristinare il cleanup di sicurezza.

Quando si utilizza CA Cleanup con CA ACF2™, è possibile identificare gli ID di login, come pure i set di regole e le singole regole, attivi o inattivi; sono incluse le classi di risorse definite dall'utente e le regole NEXTKEY source e target. Quando si utilizza CA Cleanup con CA Top Secret®, è possibile identificare gli ACIDS, le autorizzazioni e le connessioni di profilo attivi o inattivi; sono incluse le risorse definite dagli utenti e i record *ALL*. Quando si utilizza CA Cleanup con IBM® RACF®, è possibile identificare gli ID utente, i profili, le autorizzazioni, le connessioni di gruppo e i gruppi di risorse IBM RACF attivi o inattivi; l'utilizzo delle autorizzazioni viene tracciato fino alla singola voce di accesso, distinta, generica o condizionale che sia.

CA Compliance Event Manager

CA Compliance Event Manager fornisce monitoraggio di sicurezza proattivo contribuendo inoltre a ridurre costo, complessità e sforzi necessari per monitorare e segnalare i problemi di compliance e sicurezza. Con più componenti pensate per elaborare informazioni sugli eventi di utilità di gestione della sicurezza esterni e per monitorare senza soluzione di continuità i sistemi in relazione alle modifiche alle risorse critiche, CA Compliance Event Manager genera avvisi, analizza e protegge i dati mainframe mission-essential, per fornire agli stakeholder principali informazioni in tempo reale sulle violazioni potenziali della sicurezza.

Una parte importante della compliance con il GDPR si focalizzerà sulla modalità della raccolta futura dei dati; ma una notevole enfasi verrà posta sui dati già in possesso delle aziende. Data la presenza di molti mainframe che contengono dati vecchi di generazioni, un controllo manuale dei dati è assolutamente impensabile. È qui che entra in gioco CA Compliance Event Manager, con le sue tre funzionalità critiche:

- **Avvisi.** La soluzione consente di monitorare interi sistemi di record di sicurezza, punti di configurazione di sicurezza, set di dati di sistema e controlli di configurazione IBM z/OS® con notifiche in tempo reale e immediate di violazioni pertinenti, accesso e attività di modifica a sistemi e risorse di sicurezza critici. Questo consente agli stakeholder di ottenere immediatamente informazioni critiche sul potenziale e sul livello dell'esposizione dei dati sul mainframe, per prevenire in modo proattivo eventi di sicurezza negativi.
- **Analisi.** Una volta individuate le minacce all'esposizione dei dati, CA Compliance Event Manager genera informazioni avanzate di controllo e di compliance, non disponibili nei report di sicurezza standard. Grazie alla sua sofisticata raccolta dati, a un controllo completo dei dati e al supporto dei data warehouse, la soluzione consente agli utenti di riprodurre tutti gli eventi di sicurezza, di eseguire l'analisi forense a partire dalla registrazione e dalla ricerca dei dati di sicurezza grezzi, di filtrare e analizzare i dati storici registrati con il recupero automatico dei nastri, il tutto per fornire informazioni di dettaglio sui problemi di sicurezza e di compliance, nonché una condizione di rischio migliorata.
- **Protezione.** Una volta ricevute le notifiche in tempo reale e verificate le esposizioni dei dati per diagnosticare rapidamente qualsiasi problema, si dispone di un miglior controllo sui dati mainframe e si è più preparati a stabilire chi ha accesso ai dati interessati dal GDPR, dai dipendenti ai clienti ai partner di business, presenti e passati, per garantire che siano applicate le autorizzazioni appropriate.

Sezione 4:

Conclusioni

La compliance con il GDPR può essere ottenuta attraverso una combinazione di persone, processi e tecnologia. Questo documento illustra soluzioni che possano aiutare le aziende nel loro percorso verso la compliance con il GDPR. Ma è possibile estendere la protezione e rafforzare ulteriormente i controlli di sicurezza attraverso l'autenticazione forte e del rischio o la workload automation, per automatizzare l'elaborazione dei dati personali, facilitando il rispetto del GDPR e di normative analoghe. Le normative tendono a stabilire i requisiti minimi richiesti ma, nell'application economy, le aziende aperte devono garantire la due diligence per proteggere una delle risorse più importanti e critiche: le informazioni private dei clienti.

È importante non guardare al GDPR in isolamento, ma nel contesto di molte altre leggi e normative, comprese quelle specifiche di settore, che si concentrano sulla protezione dei dati nell'application economy. Controlli forti per la sicurezza e la protezione dei dati e in materia di utilizzo e accesso degli stessi saranno fondamentali per la compliance con queste leggi e normative da parte delle aziende, a prescindere dal settore.

Consulta i seguenti materiali per saperne di più sulle soluzioni CA Technologies e sul GDPR:

- E-book: "Compliance con il Regolamento generale sulla protezione dei dati dell'Unione Europea. Le implicazioni per il Test Data Management"
- White paper: "Regolamento generale sulla protezione dei dati dell'Unione Europea (GDPR): Sei pronto?"

Entra in contatto con CA Technologies all'indirizzo ca.com/it

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di cogliere le opportunità offerte dall'application economy. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, fino alla gestione e alla sicurezza, CA Technologies collabora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobile, cloud pubblici e privati, distribuiti e mainframe. Per ulteriori informazioni, visita il sito ca.com/it.

CS200-255926_0217