ManageEngine
EventLog Analyzer

Tutto ciò che devi sapere e fare per essere conforme al regolamento generale UE sulla protezione dei dati

Indice

Introduzione

L’aumento del numero, della portata e del costo delle violazioni di dati ha costretto i governi del mondo ad attuare severe leggi di conformità per proteggere i dati personali dei cittadini. L’Europa non fa eccezione. Dal 2012, la Commissione Europea ha inquadrato nuove protezioni dei dati che possono migliorare i metodi di trattamento dei dati, aumentare la protezione dei dati, e portare anche armonizzazione nella protezione di dati sensibili in tutte le nazioni europee.

Grazie a diverse modifiche apportate alle regole esistenti di protezione dei dati, il nuovo regolamento generale sulla protezione dei dati (GDPR) sta attirando maggiore attenzione. La struttura di GDPR dell'UE è complessa da implementare, con nuovi criteri in materia di responsabilità, procedure di notifica di violazioni e regole severe per il flusso internazionale di dati. Con soli pochi mesi rimasti per conformarsi a questo nuovo regolamento, è il momento giusto per le organizzazioni per rivisitare le loro strategie di protezione.

Questa guida evidenzia i cambiamenti, le sfide e i piani di azione chiave che le organizzazioni dovrebbero adottare per assicurare la compliance al GDPR.

Cambiamenti, requisiti e piani di azione

GDPR non ha confini

Il GDPR è una legge globale per la protezione dei dati che si estende oltre le aziende che operano solo in UE. Qualsiasi organizzazione che ha come target i consumatori nell'UE, tratta i dati personali di cittadini UE o monitora il comportamento dei soggetti interessati dell'UE deve attenersi ai requisiti del GDPR.

Requisiti:

- È il momento di rivisitare i quadri di sicurezza e le politiche delle società. Le organizzazioni che non operano nell'UE ma che si occupano di dati UE dovranno adottare misure per conformarsi al nuovo GDPR.
- Le organizzazioni che operano in UE e che sono conformi alla legge esistente dell'UE sulla protezione dei dati devono anch'esse rivisitare il loro quadro di sicurezza per assicurare la soddisfazione dei requisiti rigorosi del nuovo GDPR.

I piani di azione

- Se la propria organizzazione fornisce merci o servizi o monitora il comportamento di cittadini basati in UE, è necessario conformarsi ai requisiti del GDPR entro il 25 maggio 2018.
- Rivisitare le proprie politiche sulla sicurezza e assicurarsi di aver adottato le misure idonee come indicato di seguito nel trattamento dei dati personali.
- Redigere note sulla privacy e altri documenti idonei che possono essere utilizzati per ottenere il consenso esplicito e chiaro da individui per il trattamento dei loro dati personali. Se si dispone già di tali documenti, considerare di rivisitarli e rivederli in accordo con il nuovo regolamento.
- Monitorare le misure tecniche e organizzative adottate per assicurare la privacy e la sicurezza dei dati personali raccolti.
  Se necessario, incaricare responsabili che possono monitorare i processi dei dati e chi è responsabile per la sicurezza dei dati personali e sensibili.

Contenuto dei dati personali esteso

Il nuovo regolamento amplia la definizione dei dati personali e dei dati personali sensibili.

Secondo il GDPR, i dati personali sono "qualsiasi informazioni relativa a una persona naturale identificata e identificabile". Includono anche "identificatori online" come identificatori di indirizzi IP e di cookie.

Oltre alla definizione dei dati personali, il GDPR classifica alcuni dei dati personali come dati personali sensibili. Secondo il GDPR, i dati personali sensibili sono "qualsiasi dato relativo all'origine razziale o etnica, opinioni politiche, credenze religiose o filosofiche, associazioni sindacali, salute o vita sessuale e dati genetici e biometrici".

I nuovi requisiti impongono inoltre che le organizzazioni ottengano un consenso valido dai "soggetti interessati" prima di trattare i loro dati personali.

Sfide:

- Quest'ampia definizione dei dati personali e l'inclusione dell'"identificatore online" costringe le organizzazioni che si occupano di analisi dei dati, analisi comportamentali, pubblicità, e social media a conformarsi al GDPR.

I piani di azione

- Definire l'ambito dei dati di cui si occupa la propria organizzazione.
- Se i dati si adattano alla definizione di GDPR di "dati personali", allora preparare una nota o documento sulla privacy che richiede il consenso esplicito e chiaro degli individui per il successivo trattamento dei dati.
- Se si sta già cercando il consenso per trattare i dati, considerare di rivisitarli e rivederli in accordo con i nuovi requisiti di compliance.

Principi di protezione dei dati ridefiniti

Il principio di protezione dei dati che forma la spina dorsale dei requisiti di GDPR rimane lo stesso di quello indicato nella legge sulla protezione dei dati, il regolamento di compliance precedente, con alcuni ulteriori elementi aggiunti al suo interno.

I sei principi di protezione dei dati indicano che i dati personali e i dati personali sensibili devono essere,

- Trattati equamente, nel rispetto delle leggi e in modo trasparente.
- Raccolti per scopi specificati, espliciti e legittimi e non devono essere trattati in modo incompatibile con gli scopi sopra citati. L'ulteriore archiviazione dei dati per interesse pubblico o scientifico, storico o scopi statistici non deve essere considerata incompatibile con gli scopi iniziali.
- Adeguati, pertinenti e limitati a ciò che è necessario in relazione allo scopo per cui sono trattati.
- Accurati e aggiornati. Devono essere adottate procedure per cancellare o rettificare i dati personali che risultano inaccurati.
- Mantenuti in una forma che permette l'identificazione dei soggetti interessati per non più del necessario agli scopi per il quale sono trattati. Possono essere archiviati per un periodo più lungo solo se l'archiviazione supporta interessi pubblici o finalità scientifiche, storiche o statistiche. Inoltre, le organizzazioni devono adottare misure tecniche per salvaguardare i diritti e la libertà degli individui.
- Trattati con misure tecniche e organizzative appropriate che assicurino adeguata protezione dal trattamento illecito, perdita accidentale, distruzione o danneggiamento.

Il nuovo GDPR indica severi requisiti di responsabilità che rendono i responsabili dei dati a) responsabili di assicurare che siano in atto principi di protezione dei dati e b) dimostrare che l'organizzazione si attiene al GDPR.

Requisiti:

- Oltre a soddisfare i principi di protezione dei dati come tali, le società dovrebbero chiaramente definire il loro ruolo nel trattamento dei dati (vale a dire, responsabili o incaricati del trattamento) e abbracciare le loro responsabilità in accordo al nuovo regolamento.
- Le organizzazioni dovrebbero rivedere il loro flusso di audit dei dati per soddisfare i nuovi requisiti di responsabilità del GDPR.

- Un nuovo approccio basato sul rischio dovrebbe essere adottato dalle società se stanno trattando dati personali ad alto rischio. I responsabili dei dati devono effettuare valutazioni dell'impatto della protezione dei dati (DPIA) per accertare il rischio associato ai dati personali persino prima di elaborarli. Il DPIA consente inoltre l'identificazione e la prevenzione delle violazioni dei dati a una fase iniziale in modo da ridurre il danno in termini di costo che potrebbe verificarsi.
- Quando un progetto che si occupa di dati personali viene iniziato, le organizzazioni dovrebbero abbracciare un approccio di "privacy by design" per ridurre il rischio di violazioni dei dati.

I piani di azione

- Documentare tutte le informazioni relative all'elaborazione dei dati, includendo:
    - Quale tipo di dati personali viene raccolto.
    - Come vengono raccolti, usati, trasmessi e
    - conservati.

      Come vengono protetti dalla divulgazione in ciascuna fase.
- Oltre a documentare informazioni includendo dove vengono conservati i dati e chi possiede i dati, le società dovrebbero costantemente monitorare attività come:
    - Chi accede ai dati personali.
    - Con chi sono condivisi i dati.
- Monitorare continuamente il file o la cartella dove sono conservati i dati, in modo da identificare e segnalare istantaneamente qualsiasi tentativo di accesso non autorizzato o illecito.
- Mantenere un registro di quanto tempo devono essere conservati i dati. E mentre sono conservati, assicurarsi che i dati siano criptati e a prova di manomissione.

Responsabilità

Ogni organizzazione che tratta dati personali o sensibili agisce da responsabile o da soggetto incaricato al trattamento. Per assicurare la responsabilità, il GDPR raggiunge il corretto equilibrio tra i ruoli dei responsabili e degli incaricati del trattamento, rendendoli parimenti responsabili di essere conformi.

Responsabili dei dati

- Secondo il GDPR, “I responsabili sono qualsiasi entità che, da sola o unitamente ad altre, determina come e perché i dati personali vengono trattati”.
- I responsabili hanno il compito di:
  - Rivedere tutte le attività di trattamento dei dati.
  - Mantenere la documentazione pertinente di tutte le attività di trattamento dei dati.
  - Condurre valutazioni del rischio della protezione dei dati per processi ad alto rischio.
  - Implementare la protezione dei dati intrinseca e predefinita.
  - Incaricare responsabili dei dati e definire istruzioni su come trattare i dati.
  - Notificare alle autorità in caso di qualsiasi violazione dei dati.

Incaricati al trattamento dei dati

- Secondo il GDPR un incaricato al trattamento dei dati è "qualsiasi persona (diversa dal dipendente del responsabile del trattamento dei dati) che tratta i dati per conto del responsabile del trattamento dei dati".

  Gli incaricati del trattamento dei dati fanno quanto segue:

  - Trattano i dati solo con istruzioni documentate da parte del responsabile dei dati.
  - Impiegano misure di sicurezza e organizzative per evitare violazioni dei dati.
  - Eliminano tutti i dati personali al termine del trattamento e con l'istruzione da parte del responsabile.
  - Mantengono un registro scritto di attività di trattamento effettuate per conto dei responsabili.
  - Nominano un Responsabile della protezione dei dati (DPO) ove richiesto.
  - Notificano immediatamente ai responsabili in occasione di violazioni di dati.
  - Forniscono ai responsabili tutte le informazioni necessarie per dimostrare la compliance e consentire la conduzione di controlli da parte del responsabile.

Requisiti:

- Le aziende devono correggere e riesaminare i loro contratti esistenti per il trattamento dei dati per soddisfare i requisiti di responsabilità modificati. Qualsiasi nuovo contratto deve attenersi a i nuovi requisiti di GDPR.
- Sia gli incaricati sia i responsabili del trattamento devono rivisitare le loro politiche sulla sicurezza, controllo e violazione dei dati per soddisfare i nuovi requisiti del GDPR.
- Le organizzazioni devono conservare i registri delle misure adottate per prevenire violazioni dei dati.

I piani di azione

- Mantenere un chiaro registro del flusso di dati all'interno dell'organizzazione, come viene effettuata la raccolta dei dati, l'accesso, la condivisione e chi è il titolare.
- Formulare politiche sulla privacy che potrebbero evitare violazioni di dati. Questo include:
  - Monitorare la rete dell'organizzazione per rilevare eventuali anomalie.
  - Tener traccia dei comportamenti degli utenti, in particolare degli utenti privilegiati che hanno accesso per trattare i dati personali.
  - Controllare il file e la cartella in cui vengono memorizzati i dati personali. Ottenere informazioni istantanee ogni volta che è presente qualsiasi tentativo di accesso inappropriato o non autorizzato ai dati personali.
  - Assicurare misure organizzative e tecniche adeguate per salvaguardare la rete aziendale da attacchi e minacce.

Notifica di violazione dei dati

Il GDPR definisce una violazione dei dati personali come "una violazione di sicurezza che porta alla distruzione, perdita, alterazione, divulgazione non autorizzata di, o accesso a, dati personali".

Questo spiega che una violazione dei dati è più di una semplice perdita di dati. Il regolamento costringe inoltre le organizzazioni a segnalare violazioni di dati "senza ingiustificato ritardo, e ove fattibile", entro 72 ore.

Requisiti:

- Le imprese dovrebbero avere una corretta procedura interna di segnalazione delle violazioni.
- Le organizzazioni devono condurre revisioni delle supply chain e controlli regolari per assicurare di soddisfare i nuovi requisiti di sicurezza.
- Le aziende dovrebbero far uso di un sistema tecnico e di sicurezza adeguato che faciliti il rilevamento istantaneo di violazioni di dati. Il sistema dovrebbe inoltre fornire informazioni approfondite per accelerare la risposta o contenere la violazione a una fase iniziale.

I piani di azione

- Identificare gli indicatori di compromissioni (IOC) che causano le violazioni di sicurezza nella rete e preparare criteri di sicurezza per difenderle.
- Fare uso di sistemi di sicurezza come firewall e IDS/IPS che potrebbero aiutare a prevenire attacchi alla sicurezza.
- Considerare di implementare soluzioni per la sicurezza per organizzazioni che possono rilevare istantaneamente, avvisare e segnalare violazioni della sicurezza. Inoltre, le soluzioni dovrebbero essere in grado di avvisare in tempo reale ogni volta che si verifica qualsiasi perdita di dati o tentativo di violazione.
- Stabilire criteri di sicurezza che aiutano ad assicurare l'integrità dei dati identificando:
  - Accesso o tentativi di accesso non autorizzati
  - Eliminazione non autorizzata
  - Condivisione non autorizzata
  - Copia non autorizzata o tentativi di copiare dati personali
- Monitorare il comportamento di utenti privilegiati (ovvero, utenti che hanno accesso ai dati personali) per identificare attività anomale in caso di furto di identità e segnalarli immediatamente.

I diritti dei soggetti interessati

Qualsiasi azione che è possibile effettuare con i dati viene reputata trattamento di dati. Tuttavia, il GDPR definisce limiti severi a ciò che le organizzazioni possono e non possono fare con le informazioni personali che raccolgono.

Diritto di essere informati: Inizia dal punto della raccolta dei dati. Le organizzazioni devono informare i soggetti dei dati che le informazioni raccolte da loro saranno trattate in modo trasparente ed equo, tramite una nota sulla privacy. Inoltre, è un obbligo per le imprese di ottenere un consenso chiaro e valido dai soggetti interessati per elaborare le loro informazioni personali tramite un documento di consenso redatto in termini semplici.

Diritto di accesso: Ai soggetti dei dati o individui deve essere fornito il diritto di accedere alle loro informazioni personali in qualsiasi momento. Con questo requisito, il GDPR assicura che gli individui abbiano il diritto di controllare e convalidare che le loro informazioni siano trattate equamente.

Diritto alla rettifica: Se gli individui reputano che i loro dati personali siano incompleti o non accurati, hanno il diritto di chiedere all'impresa di rettificare i loro dati personali. Quando è stata formulata una richiesta di rettifica, è responsabilità del responsabile del trattamento dei dati di fornire informazioni agli individui interessati sulle azioni intraprese per la richiesta, senza ritardo ingiustificato.

Diritto a limitare il trattamento dei dati: Quando il trattamento dei dati è limitato, il responsabile può solo archiviare i dati personali e non può eseguire alcun tipo di trattamento sui dati. Gli individui possono limitare il trattamento dei loro dati se:

- Viene scoperto che i dati sono incompleti o non accurati.
- I dati sono trattati in modo illecito.
- Il responsabile non ha più alcun motivo (in accordo con i principi di protezione dei dati) per trattare i dati personali.

Diritto alla portabilità dei dati: Gli individui, in qualsiasi momento, senza alcun impedimento, possono ottenere i loro dati e trasferirli a un altro responsabile per il trattamento. Questo diritto consente agli individui di spostare, copiare, trasferire dati personali in modo semplice da un ambiente a un altro in modo sicuro.

Diritto all'oblio: Il GDPR concede pieni diritti agli individui di richiedere l'eliminazione o la rimozione dei loro dati personali. La richiesta di cancellazione dei dati può essere formulata in queste circostanze:

- Laddove la conservazione dei dati personali non sia più necessaria in relazione allo scopo per cui sono stati originariamente raccolti o trattati.
- Quando il soggetto ritira il consenso al trattamento dei dati.
- Quando il soggetto interessato formula una richiesta di terminare il trattamento dei dati a causa del trattamento illecito dei dati o se si è verificata una violazione dei dati.
- Se i dati devono essere cancellati per scopi di conformità a un obbligo giuridico.

I piani di azione

- Redigere un modulo di richiesta di consenso o nota sulla privacy adeguati che possano ottenere il chiaro ed esplicito consenso da individui per trattare dati personali.
- Documentare le tecniche di trattamento e i flussi di trattamento dei dati così da poterli fornire agli individui quando li cercano attraverso il loro diritto all'accesso.
- Adottare misure tecniche per cancellare automaticamente dati personali dopo che il relativo scopo è stato conseguito.
- Mentre i dati vengono conservati, assicurarsi che la loro integrità sia preservata cifrando i dati.
- Documentare le informazioni di cifratura per fornirle ai soggetti interessati, se necessario.

Sanzioni per violazione della compliance

Quando le organizzazioni non sono conformi al GDPR o violano i requisiti del GDPR, gli amministratori possono imporre una sanzione fino a **€10 milioni oppure il 2% del fatturato annuale della società in tutto il mondo nell'anno finanziario precedente,** qualunque importo sia superiore. I responsabili e gli incaricati al trattamento dei dati sono passibili di questa enorme multa quando le condizioni seguenti vengono violate:

- Principi di protezione dei dati fondamentali
- Condizioni per il trattamento di dati non personali
- Condizioni per il consenso
- Condizioni per il trattamento dei dati personali sensibili
- Diritti dei soggetti interessati

Il commissario per la protezione dei dati personali che impone la multa prende in considerazione la natura e l'intensità della violazione, le misure di prevenzione intraprese, misure tecniche e organizzative implementate e altro per decidere l'importo della sanzione.

Soddisfare i requisiti di conformità GDPR con le soluzioni di sicurezza IT di ManageEngine

Il portfolio di soluzioni di sicurezza IT di ManageEngine include un'ampia gamma di strumenti che consentono alle organizzazioni di garantire la conformità alle direttive GDPR. La nostra suite comprende:

- **Log360**, un avanzato strumento SIEM che consente alle organizzazioni di rilevare violazioni dei dati, garantire la sicurezza dei dati personali archiviati e tenere traccia dell'accesso ai dati personali, in modo da assicurare il rispetto dei requisiti di responsabilità.
- **File Audit Plus**, uno strumento di controllo e monitoraggio dei file in tempo reale che aiuta a tenere traccia di qualsiasi modifica di importanza critica apportata ai file e alle cartelle che contengono dati personali.

In che modo le nostre soluzioni consentono di soddisfare i requisiti GDPR

- **La misura tecnica e organizzativa per difendere o prevenire violazioni della sicurezza:** Utilizzare Log360 e File Audit Plus può essere la misura tecnica che le organizzazioni adottano per difendere o prevenire violazioni della sicurezza. Queste soluzioni hanno la capacità di monitorare le attività di tutti i dispositivi e utenti nella rete e segnalano istantaneamente le anomalie agli amministratori. Il professionista della sicurezza può quindi indagare l'incidente con i report esaustivi e, se viene scoperto che l'incidente è una violazione della sicurezza (o un tentativo di violazione), potrà adottare misure immediate per contenerlo già in fase iniziale.
- **Controllo dei dati:** La funzione di monitoraggio in tempo reale dell'integrità dei file di File Audit Plus monitora continuamente le modifiche ai dati critici. Fornisce inoltre informazioni dettagliate su chi ha avuto accesso ai dati, quando è stato eseguito l'accesso e da dove. Questo report dettagliato aiuta a fornire informazioni ai soggetti interessati sugli accessi ai dati e monitora anche i flussi di dati.
- **Conduzione di audit trail:** La potente funzionalità di ricerca nel registro di Log360 aiuta a condurre agevolmente l'analisi forense. Uno dei requisiti del GDPR è la capacità di scoprire la causa principale della violazione o del tentativo di violazione dei dati, in modo da risolvere istantaneamente il problema. La nostra soluzione può aiutare a individuare la causa principale di una violazione dei dati eseguendo ricerche all'interno di terabyte di dati dei registri in pochi minuti. La soluzione fornisce inoltre la possibilità di esportare i risultati della ricerca in un report forense, in modo da poterli inviare ai DPO. La query di ricerca può anche essere convertita in un profilo di avviso per prevenire futuri attacchi alla sicurezza dello stesso tipo.

- **Soddisfare il requisito PIA/DPIA:** I report dettagliati e i profili di avviso di Log360 rilevano istantaneamente qualsiasi anomalia di rete e i tentativi di violazione della sicurezza. Questo aiuta a contenere la violazione dei dati già in fase iniziale e riduce al minimo il danno per i dati e il costo altrimenti subito, soddisfacendo quindi il requisito PIA/DPIA del GDPR.

- **Requisito di notifica di violazione:** Log360 invia agli amministratori avvisi e-mail o SMS in tempo reale su violazioni dei dati. Questo li aiuta a segnalare la violazione ai responsabili di grado più elevato senza ritardo ingiustificato. La soluzione include oltre 600 profili di avviso predefiniti che sono basati su vari IOC. Questo aiuta a rilevare i tentativi di violazione istantaneamente e con la massima facilità. Inoltre, la soluzione fornisce la possibilità di creare profili di avviso personalizzati per soddisfare le esigenze di sicurezza interne.

Informazioni su ManageEngine

ManageEngine offre gli strumenti di gestione IT in tempo reale che consentono a un team IT di soddisfare una necessità dell'organizzazione per servizi e supporto in tempo reale. In tutto il mondo, oltre 60.000 imprese avviate ed emergenti, incluso oltre il 60% del Fortune 500, si affidano ai prodotti di ManageEngine per assicurare le prestazioni ottimali della loro infrastruttura IT critica, tra cui reti, server, applicazioni, desktop e altro. ManageEngine è una divisione di Zoho Corp., con uffici in tutto il mondo, inclusi gli Stati Uniti, il Regno Unito, l'India, il Giappone e la Cina.

Informazioni sull'autore

Subhalakshmi Ganapathy lavora attualmente come Analista senior di Marketing prodotti per soluzioni di sicurezza IT presso ManageEngine. Dispone di una conoscenza approfondita della sicurezza delle informazioni e della gestione della compliance. Fornisce una guida strategica per imprese sulla Gestione di informazioni ed eventi sulla sicurezza (SIEM), sicurezza di rete e privacy dei dati.

Contattare Subha all'indirizzo subhalakshmi.g@manageengine.com.

E-mail:
support@eventloganalyzer.com

In alternativa

Chiamare il numero verde:

Stati Uniti: +1 888 720 9500 Regno Unito: 0800 028 6590

Australia: +1 800 631 268 Cina: +86 400 660 8680

Internaz.: +1 925 924 9500

In alternativa

Visitare www.eventloganalyzer.com per informazioni approfondite sulla soluzione e tutte le sue funzionalità.