ASSIMEA
ASSOCIAZIONE ITALIANA DELLE IMPRESE

SECURITY LOGIC

PREPARARSI AL NUOVO REGOLAMENTO PER LA PROTEZIONE DEI DATI (GDPR)

SECURITY LOGIC

Premessa

Il nuovo Regolamento Europeo sulla Protezione dei Dati (GDPR) rilasciato per tutti gli stati membri il 24 Maggio 2016 è entrato definitivamente in vigore anche in Italia.

Il regolamento comporta una serie di innovazioni non solo per il singolo cittadino ma anche per aziende, enti pubblici, liberi professioni ed associazioni.

Indipendentemente dal ramo aziendale, Risorse umane, Marketing, Legale o IT, il cambiamento riguarderà ogni dipendente e avrà un impatto sulla sua giornata lavorativa.

L'azienda che possiede o utilizza dati personali, ad esempio dati dei dipendenti o di clienti diretti o potenziali, dovrà adeguare la propria organizzazione e i processi che la governano ai cambiamenti introdotti dal nuovo regolamento per garantire l'integrità dei dati e il loro utilizzo in conformità al livello di consenso correttamente acquisito.

Quali sono i principali cambiamenti

Il nuovo regolamento per il trattamento dei dati personali richiede alle aziende di acquisire piena consapevolezza di quali e quante sono le informazioni personali gestite, dove si trovano e come e in quali transazioni vengono utilizzate.

I PUNTI CHIAVE DEL REGOLAMENTO	PAROLE CHIAVE
1. Tutti i dati personali che controllati e/o gestiti, a prescindere che vengano elaborati nell'UE o meno, dovranno essere trattati in modo equo e trasparente, con un utilizzo chiaro nei confronti dei soggetti a cui i dati appartengono (ovvero i cittadini).	TRASPARENZA
2. Nel caso di violazione delle normative, saranno applicate sanzioni pecuniarie severe con un valore fino al 4% del fatturato globale annuale o € 20 milioni (quello che risulterà essere il valore maggiore)	SANZIONI E VINCOLI
3. Le violazioni dei dati devono essere notificate entro 72 ore dal momento in cui il gestore dei dati ne viene a conoscenza.	
4. Sarà necessario un consenso più rigoroso per l'utilizzo dei dati, agevolando ai cittadini la possibilità di revoca di tale consenso qualora lo desiderino.	CONSENSO ESPLICITO
5. I soggetti interessati godranno di diritti più ampi per ottenere informazioni su modalità, posizione e scopi dell'elaborazione dei propri dati.	DIRITTI E GARANZIE
6. La cancellazione dei dati (o "il diritto all'oblio") sarà semplificata, con i soggetti proprietari dei dati che potranno richiedere la cancellazione o l'interruzione del trattamento dei propri dati (dimostrando che la richiesta soddisfa determinate condizioni).	
7. Sarà abilitata la portabilità dei dati, che conferisce ai soggetti proprietari dei dati il diritto di ricevere i dati personali che li riguardano.	
8. I processi di elaborazione dei dati (o "Privacy by design") devono essere inclusi fin dalle fasi iniziali della progettazione dei nuovi sistemi, piuttosto che aggiunti in un secondo momento.	
9. Sarà obbligatoria la presenza di responsabili della protezione dei dati (DPO) per le aziende la cui attività consiste in operazioni di elaborazione che richiedono un monitoraggio regolare e sistematico dei contenuti dei dati dei soggetti interessati su larga scala o in alcuni casi in cui vengono elaborati volumi significativi di dati di "categoria speciale".	RESPONSABILITA' DI GESTIONE DEI DATI

Come si diventa GDPR Compliance

Con l'obiettivo di semplificare il percorso che l'azienda deve seguire per allinearsi alle nuove richieste del regolamento abbiamo schematizzato il processo in 5 passi :

CONSAPEVOLEZZA (SCOPERTA)
E' opportuno conoscere tutte le VULNERABILITA' dell'azienda avviando una indagine approfondita dei vari sistemi interni ed esterni per avere piena consapevolezza delle fragilità e dei rischi a cui si è esposti.
La mappatura dei dati è necessaria per analizzare la portabilità dei dati, i diritti di accesso e di cancellazione…
E' necessario identificare e classificare i dati personali…

PROTEZIONE & REVISIONE
La pseudonimizzazione e la cifratura dei dati personali.
La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Le procedure per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative adottate.
E' fondamentale considerare il diritto delle persone di tracciare, modificare, cancellare e trasferire i dati.
E' necessario implementare strumenti per dimostrare che le richieste vengano processate in modo corretto.

CONTROLLO & REPORTING
Viene richiesta la capacità di segnalare eventuali violazioni entro 72 ore dall'avvenimento.
La comunicazione deve contenere: La descrizione della violazione, la natura dei dati interessati, le probabili conseguenze della violazione, le misure adottate per porrerimedio.
E' necessario dotarsi di strumenti che

SPHERE Concept : GDPR Engine e protezione del rischio

SECURITY LOGIC ha sviluppato un concetto di sicurezza globale per la gestione dei dati personali che comprende il **controllo dell'infrastruttura IT** e la **garanzia assicurativa** di copertura del rischio derivante da eventuali attacchi informatici.

La piattaforma Sphere è una soluzione modulare, completamente scalabile che eroga i servizi in modalità SaaS (Software as a Service) ed è gestita completamente in Cloud.

SPHERE raccoglie dati da host eterogenei e controlla apparati di brand differenti attraverso un'unica interfaccia con l'obiettivo di gestire da un unico punto l'intera rete aziendale.

SPHERE è composta da quattro moduli tra loro indipendenti ma che operano in modo complementare per garantire la conformità ai requisiti del nuovo Regolamento.

Per ottemperare alle necessità previste dalla normativa è necessario dotarsi di efficaci strumenti di raccolta e gestione dei LOG relativi al trattamento dei dati, al loro monitoraggio e alla correlazione di eventi per verificare in anticipo ogni tentativo di violazione. I moduli di **Gestione dei Log**, **Correlazione Eventi** e **Monitoraggio Attivo** garantiscono il controllo istantaneo e continuo dell'accesso ai dati attraverso il tracciamento di ogni transazione.

Il modulo di **Scansione delle Vulnerabilità** permette di verificare con continuità eventuali punti deboli del sistema di sicurezza implementato a protezione dei dati personali.

La protezione del rischio residuo

La diffusione pervasiva di strumenti digitali rende gli attacchi informatici un pericolo sempre più evidente e sentito.
Allo stesso tempo, nonostante la tecnologia giochi un ruolo determinante nelle aziende, la maggior parte di esse, a prescindere dal settore di appartenenza, non comprende a fondo i rischi a cui è esposta finché non si verifica un problema.
In realtà si può affermare che nessun sistema è immune da interruzioni informatiche e da attacchi, e un sinistro cyber, se non gestito correttamente, può compromettere non solo l'immagine dell'azienda, ma anche il suo bilancio.

Valutare il rischio

Le compagnie assicurative sono tenute ad effettuare una VALUTAZIONE DI IMPATTO al fine di poter effettuare correttamente l'assunzione del rischio di copertura, attraverso:

- Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento
- Una valutazione delle necessità e proporzionalità dei trattamenti in relazione delle finalità
- Una valutazione dei rischi per i diritti e le libertà degli interessati
- Le misure previste per affrontare i rischi

Le informazioni chiave per la valutazione del rischio

All'azienda viene chiesto di fare un attento esame della propria cyber postura e questo percorso tocca sempre i seguenti aspetti:

- Quanti e quali sono i dati personali gestiti
- Le policy di protezione dei dati
- La geo-localizzazione delle sedi
- Sistemi firewall e antivirus
- Monitoraggio delle intrusioni
- Transazioni con carte di credito
- Gestione della privacy
- Utilizzo della crittografia
- Sistemi di backup
- Accesso fisico ai sistemi
- Accesso da remoto
- Outsourcing di servizi informatici
- Esposizione sui social network
- Strategie di business continuity

Garanzie e coperture

La perdita di profitto per l'interruzione delle attività aziendali a seguito di attacco informatico o falle nella sicurezza della rete, errore umano o errore di programmazione.

La perdita e il ripristino dei dati, compresi decontaminazione e recupero.

- Spese per servizi di Incident Response e costi investigativi, con il supporto di una linea diretta anticrisi, multilingue e attiva 24/7
- Costi derivanti da ritardi o interruzione in caso di business interruption
- Spese legali, ivi comprese quelle per far valere le penali contrattuali
- Spese sostenute per la comunicazione in situazioni di crisi e la mitigazione del danno alla reputazione
- Responsabilità derivante dalla mancata tutela dei dati personali
- Responsabilità derivante dall'uso non autorizzato delle telecomunicazioni
- Estorsione/riscatto legato alla rete o ai dati (ove assicurabile)
- Responsabilità relativa alla gestione dei media online

La copertura assicurativa per il DPO

La figura del DPO (Data Processor Officer)svolge un ruolo particolarmente delicato ed esposto al rischio di causare danni a terzi o per inadempienze professionali causate da fatto colposo (lieve o grave) o da errori oppure da omissioni involontarie.

Pertanto con l'obiettivo di salvaguardare il DPO dal pagamento di qualsiasi somma dovuta, pur nei limiti del massimale identificato, è stata costruita una copertura specifica che copre sia il professionista che le persone di cui, nello svolgimento di tale funzione, è tenuto legalmente a rispondere.

In particolare le coperture offerte coprono i danni per:

- Violazione involontaria dei dati personali
- Diffamazione e danni di immagine o reputazionali
- Perdita di documenti e eventuale ripristino

Sono inoltre comprese la GARANZIA POSTUMA per attività svolta prima della cessazione dell'attività o dell'incarico e la RESPONSABILITA' CIVILE nella conduzione dello studio presso cui è svolta l'attività di DPO.

www.securitylogic.it
www.assimea.it
Per informazioni scrivere a:
assimea.gdpr@securitylogic.it

Sedi Operative:
L.go G. Re Umberto, 102 10128 TORINO
Via Felice Casati, 27 20124 MILANO
Via Armando Diaz, 8 80134 NAPOLI

Numero Verde 800 240 670