F-Secure

IL NUOVO PANORAMA DELLA PRIVACY

Cosa devono fare le aziende prima e dopo la scadenza di maggio 2018 per rispettare il GDPR

01 IL REGOLAMENTO GDPR IN BREVE

Il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (GDPR) entrerà in vigore a maggio 2018. La direttiva segna il cambiamento normativo più significativo in materia di protezione dei dati avvenuto nell'Unione Europea negli ultimi 20 anni e trasformerà il modo in cui le aziende gestiscono e proteggono i dati personali.

Il GDPR si applicherà al trattamento dei dati da parte dei titolari e dei responsabili del trattamento nell'Unione Europea, a prescindere dal fatto che il trattamento stesso avvenga nella UE o meno. Il regolamento si applicherà anche al trattamento dei dati personali dei cittadini dell'UE da parte di un titolare del trattamento o responsabile del trattamento non ubicato nella UE, se svolge attività correlate all'offerta di beni e servizi a cittadini UE o al monitoraggio di comportamenti che hanno luogo all'interno dell'UE.

IL GDPR È DESTINATO A:

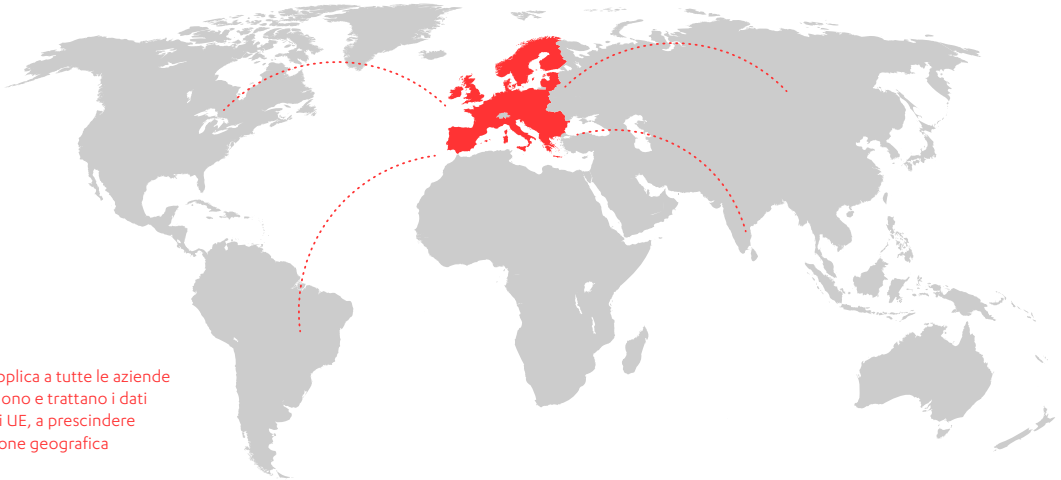
- Armonizzare le normative sulla protezione dei dati in tutta Europa
- Restituire ai cittadini UE il controllo e proteggere la privacy dei loro dati
- Ridefinire l'approccio delle aziende alla protezione dei dati

01 GDPR in breve

02 Elementi chiave per prepararsi al GDPR

03 Chi deve essere coinvolto

04 Perché la cyber security è importante



Il GDPR si applica a tutte le aziende che raccolgono e trattano i dati dei cittadini UE, a prescindere dall'ubicazione geografica

Manca meno di un anno all'entrata in vigore del GDPR e le aziende stanno appena iniziando a comprendere le implicazioni pratiche che avrà. Il regolamento imporrà nuovi obblighi, ma avrà anche dei risvolti positivi. La protezione dei dati comporterà un investimento iniziale, ma porterà anche un guadagno, non solo in termini di migliore conformità e prevenzione delle violazioni, ma anche di vantaggio competitivo. Sul lungo periodo, il GDPR potrà anche portare un cambiamento nelle best practice in diversi settori, per quanto concerne l'architettura del trattamento dei dati personali. Dopo gli sforzi profusi per raggiungere la conformità iniziale, i cambiamenti dal punto di vista del design, sia sul piano aziendale che a livello di implementazione tecnica, possono essere il modo migliore per garantire una protezione dei dati a costi contenuti a lungo termine.

Invece di concentrarsi su interventi rapidi per conformarsi al GDPR, le aziende dovrebbero guardare oltre la scadenza di maggio 2018 e focalizzare l'attenzione su miglioramenti sostenibili per identificare opportunità di business, adottando un approccio proattivo alla protezione dei dati e alla cyber security. Per fare questo è importante definire le priorità in termini di risorse, processi e persone non solo per mettersi a norma ma anche per dare vita a un programma continuativo che si trasformerà in attività di business di routine.

PRINCIPI DI PROTEZIONE DEI DATI

I principi di protezione dei dati del GDPR specificano le condizioni alle quali è consentito trattare dati personali. È quindi imperativo che le aziende si accertino che le proprie attività di trattamento dei dati si svolgano in conformità con i principi di protezione dei dati definiti nel GDPR.

Oggi le aziende raccolgono grandi quantità di dati, nonostante sempre più ricerche dimostrino che esse non comprendono o traggono alcun valore da più della metà di questi. Il GDPR può essere utilizzato per stabilire quali dati possono effettivamente essere impiegati per ottenere preziose informazioni di business, per perfezionare i processi in modo da raccogliere le informazioni giuste al momento giusto e per sviluppare un legame più forte con i clienti da cui vengono raccolti i dati. In termini semplici, si tratta di un'opportunità di miglioramento per ottimizzare la gestione dei dati personali a vantaggio tanto dell'azienda quanto degli interessati.

PRINCIPI DI PROTEZIONE DEI DATI

1. Liceità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

2. Limitazione delle finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo incompatibile con tali finalità. Un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali.

3. Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati ai casi di utilizzo a cui sono attinenti.

4. Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

5. Limitazione della conservazione

I dati personali devono essere conservati in una forma che non consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

6. Integrità e riservatezza

I dati personali devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

CONCETTI CHIAVE

Dati personali

Il Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (GDPR) si applica solo ai dati personali. Per dati personali si intendono informazioni relative a una persona fisica identificata o identificabile, ovvero l'interessato. L'interessato è una 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, o qualunque elemento caratteristico della sua identità. Secondo il GDPR, il concetto di dati personali si estende ad alcune categorie di dati online, come gli identificativi online, gli identificativi prodotti dai dispositivi, gli ID dei cookie e gli indirizzi IP.

CONCETTI CHIAVE

Categorie particolari di dati personali

Il concetto di "categorie particolari di dati personali" si riferisce ai dati personali sensibili soggetti a una protezione aggiuntiva. In generale, le aziende devono avere basi più forti per trattare i dati personali sensibili rispetto ai dati personali "normali". Le categorie speciali di dati personali includono, in via esemplificativa ma non esaustiva, i dati che riguardano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, nonché i dati relativi alla salute, i dati genetici e i dati biometrici.

DATI RELATIVI ALLA SALUTE
DATI GENETICI
DATI BIOMETRICI
DATI SU ORIGINE RAZZIALE O ETNICA
OPINIONI POLITICHE
ORIENTAMENTO SESSUALE

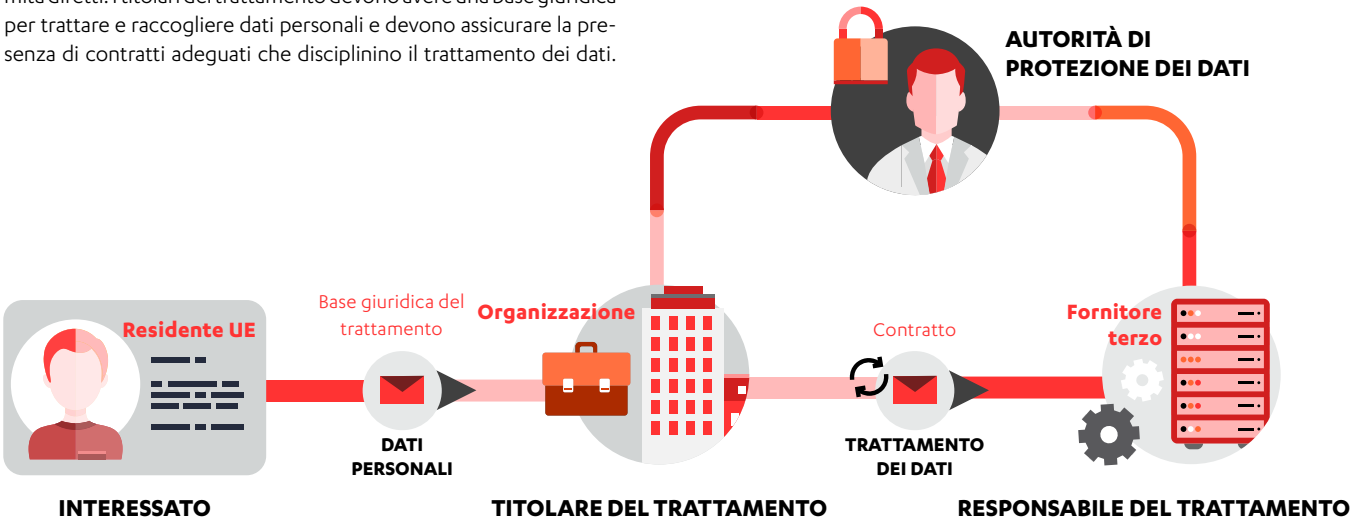
CONCETTI CHIAVE

Titolare del trattamento

Il titolare del trattamento è una persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Ai sensi del GDPR, ai titolari del trattamento spetta comunque la responsabilità principale per la conformità, anche se i responsabili del trattamento hanno anch'essi obblighi di conformità diretti. I titolari del trattamento devono avere una base giuridica per trattare e raccogliere dati personali e devono assicurare la presenza di contratti adeguati che disciplinino il trattamento dei dati.

Responsabile del trattamento

Qualsiasi persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento. Molti service provider, ad esempio, sono responsabili del trattamento dei dati. I responsabili del trattamento dei dati possono essere ritenuti direttamente responsabili della sicurezza dei dati personali.



CONCETTI CHIAVE

CONFORMITÀ
Assicurarsi di rispettare le norme

Applicare

RESPONSABILIZZAZIONE
Dimostrare di rispettare le norme

Dimostrare

GESTIONE
Proteggere costantemente i dati e monitorare la protezione

Gestire

Responsabilizzazione

Il GDPR pone l'accento sul concetto di "responsabilizzazione" nel trattamento dei dati personali. Prevede infatti che il titolare del trattamento sia tenuto a garantire che tutti i principi di privacy siano rispettati. Inoltre, il regolamento prevede che l'organizzazione possa comprovare la propria conformità a tutti i suoi principi.

La nuova legislazione incoraggia le organizzazioni a comprendere e farsi carico dei rischi che creano per gli altri, adoperandosi per attenuarli. Il GDPR intende allontanarsi dalla mera applicazione di una legge orientandosi piuttosto verso la realizzazione di un framework che possa essere impiegato per creare una cultura della protezione dei dati nell'intera organizzazione. La responsabilizzazione non può essere una clausola accessoria ma deve essere parte dell'approccio generale dell'organizzazione alla gestione e al trattamento dei dati personali.

CONCETTI CHIAVE

Consenso

Il consenso dell'interessato indica qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con la quale l'interessato manifesta il proprio assenso, mediante dichiarazione o chiara azione positiva, che i dati personali che lo riguardano siano oggetto di trattamento. Le aziende che fanno affidamento sul consenso per le proprie attività di business dovranno rivedere e rielaborare i processi mediante i quali ottengono il consenso per allinearli ai requisiti del GDPR.

Le aziende devono impegnarsi fin da ora per assicurarsi di disporre di meccanismi di consenso chiari e granulari per gli interessati. È importante che le aziende tengano presente che il consenso può essere revocato dall'interessato e questo può rappresentare un aspetto problematico perché il trattamento dei dati deve cessare lungo l'intera pipeline. Per questo motivo spesso è preferibile puntare su un'altra base per il trattamento piuttosto che fare affidamento unicamente sul consenso, a meno che non sia strettamente necessario.

Trasparenza

Le aziende dovranno fornire informazioni complete alle persone sul trattamento dei loro dati personali. Il GDPR combina diversi obblighi di trasparenza già in vigore in tutta l'Unione Europea. I titolari del trattamento dei dati devono fornire informazioni sul trattamento dei dati personali in modo conciso, trasparente, intellegibile e facilmente accessibile.

Valutazione d'impatto (PIA)

La valutazione d'impatto (PIA – Privacy Impact Assessment) è fondamentale per proteggere la privacy e la conformità dei processi e servizi al GDPR. Lo scopo della valutazione d'impatto è quello di produrre una descrizione sistematica delle attività di trattamento dei dati previste e di determinare la base giuridica per il trattamento. Le valutazioni d'impatto dovrebbero descrivere l'approccio che un'azienda adotterà per attenuare i rischi. L'esecuzione delle valutazioni d'impatto non deve essere un'attività di compliance isolata, ma incorporata nei processi esistenti in modo che i rischi potenziali e i costi riferiti alle correzioni siano chiari in fase di decisione e approvazione.

Il GDPR talvolta richiede un'attività specifica di valutazione d'impatto denominata valutazione d'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment). Il regolamento prevede l'esecuzione di valutazioni d'impatto sulla protezione dei dati per i trattamenti di dati che potenzialmente presentano un rischio elevato per i diritti e le libertà degli interessati, in particolare quando si implementano nuove tecnologie o nei casi di trattamento su larga scala di categorie particolari di dati personali. Le valutazioni d'impatto sulla protezione dei dati devono valutare la necessità e la proporzionalità del trattamento per identificare i rischi per i diritti e le libertà degli interessati. Per soddisfare i requisiti di una valutazione d'impatto sulla protezione dei dati è possibile effettuare una valutazione d'impatto più generale.

CONCETTI CHIAVE

Privacy by Design

Privacy by design significa che ogni nuovo servizio o processo aziendale che utilizza i dati personali deve prendere in considerazione la protezione di quei dati. Le aziende devono essere in grado di dimostrare che hanno adottato un adeguato grado di sicurezza e che monitorano la compliance. In pratica, questo significa che la protezione dei dati deve essere un aspetto determinante lungo l'intero ciclo di sviluppo di un nuovo sistema.

Privacy by Default

Privacy by default significa semplicemente che quando un cliente acquista un nuovo prodotto o servizio vengono applicate automaticamente le impostazioni di privacy più rigorose. In altri termini, non dovrebbero essere necessarie modifiche manuali alle impostazioni sulla privacy da parte dell'utente. I titolari o responsabili del trattamento potranno archiviare dati solo per il tempo strettamente necessario a fornire un prodotto o servizio.

Pseudonimizzazione

La pseudonimizzazione è una tecnica di protezione della privacy in cui i dati personali trattati non possono essere attribuiti a una persona specifica. A questo scopo, le informazioni vengono rese non attribuibili a una persona senza l'utilizzo di informazioni aggiuntive, che devono essere conservate separatamente e soggette a misure tecniche e controlli organizzativi. Anche se le informazioni pseudonimizzate costituiscono comunque un tipo di dati personali, il loro utilizzo è fortemente incoraggiato dal GDPR, e persino identificato come misura di sicurezza praticabile. Inoltre, possono aiutare le aziende a soddisfare i propri obblighi di "privacy by design" e "privacy by default" e possono essere utilizzate per giustificare un trattamento che altrimenti sarebbe considerato incompatibile con le finalità per cui i dati sono stati originariamente raccolti.

02 ELEMENTI CHIAVE PER PREPARARSI AL GDPR

La conformità al GDPR ha profonde implicazioni per le varie funzioni organizzative ed è per questo che la maggior parte delle aziende si sta già adoperando per modificare le proprie attività prima della scadenza di maggio 2018. Qualunque sia il processo che si decide di adottare, occorre iniziare a considerare la conformità sia in vista di maggio 2018, sia in una prospettiva futura. Se le attività di messa a norma non producono i dati e gli artefatti necessari da utilizzare in futuro, si rischia di dover rifare tutto.

1. Messa a norma

2. Conformità dopo maggio 2018

È importante che le aziende riconoscano che non tutti i rischi legati al GDPR e alla privacy sono uguali. Una violazione dei dati è un rischio nettamente diverso rispetto a una mancata conformità ai requisiti per l'accesso ai sistemi e la gestione di questi due casi può essere diversa. La procedura per la privacy dei dati dovrebbe essere in grado di distinguere i vari scenari di rischio e di prescrivere le strategie di attenuazione del rischio appropriate a seconda delle circostanze.

In generale, le aziende devono muoversi su due fronti:

A. Processi di business

I processi di business, o flussi di valore o customer journey, dovrebbero guidare i requisiti di conformità al GDPR e l'attività di conformità al GDPR a lungo termine.

B. Sistemi IT

Il lavoro a livello di sistemi dovrebbe guidare le attività di attenuazione delle violazioni dei dati.

Il collante tra questi due livelli è costituito dalla progettazione dei servizi e dall'architettura aziendale.

VISIONE AZIENDALE SULLA PRIVACY

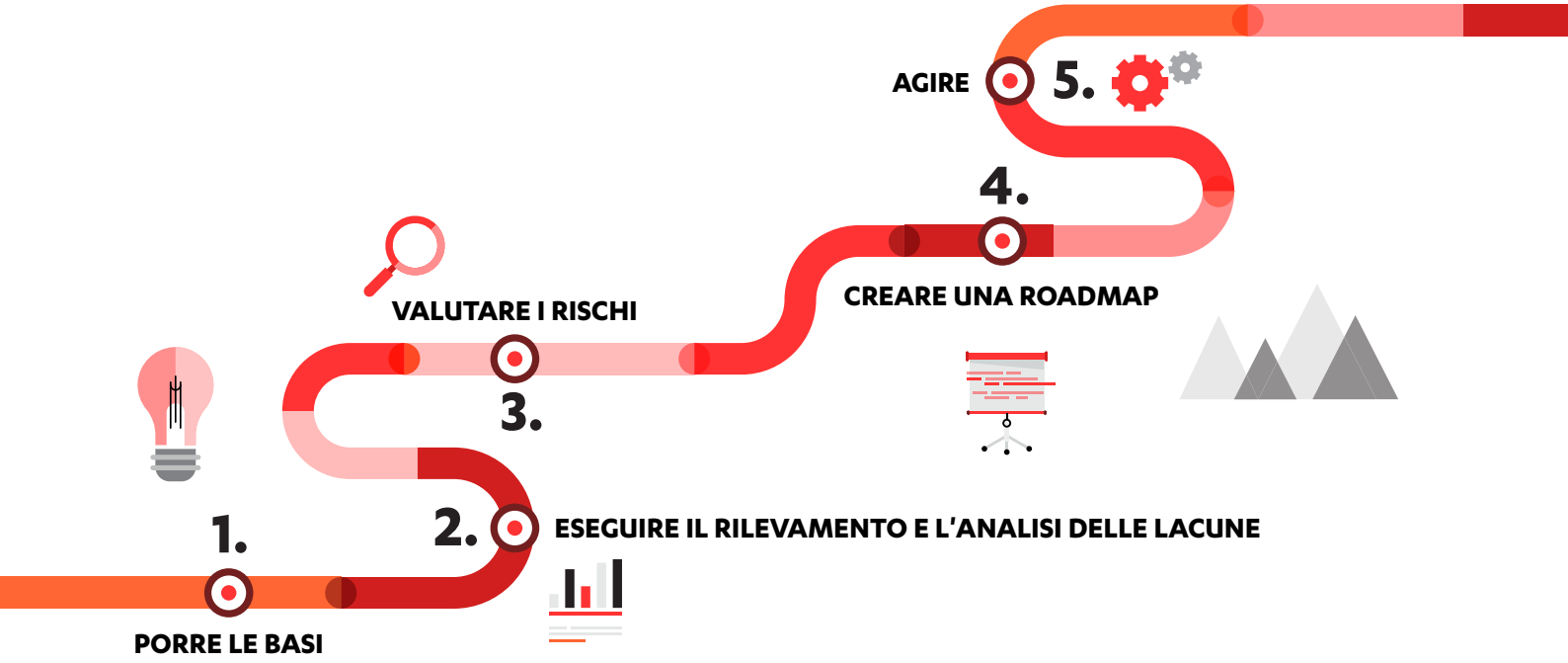
VISIONE DI GESTIONE

- Ciclo di vita dei dati, dal punto di vista di un processo o customer journey
- Descrizione e liceità del trattamento dei dati
- Diagrammi di flusso di informazioni di alto livello
- Contratti legali
- Gestione e attenuazione dei rischi quantificati

VISIONE DI SISTEMI

- Ciclo di vita dei dati, dal punto di vista dell'implementazione tecnica
- Allineamento tra implementazione tecnica e descrizione del trattamento
- Diagrammi di flusso dei dati
- API e contatti API
- Controlli di sicurezza

COME STRUTTURARE IL LAVORO PREPARATORIO?



COME STRUTTURARE
IL LAVORO PREPARATORIO

1. Porre le basi

Il primo passo da compiere è esaminare a fondo il GDPR e sensibilizzare l'organizzazione rispetto ai cambiamenti imminenti. Per adeguarsi correttamente al GDPR è essenziale ottenere l'appoggio della dirigenza e coinvolgere adeguatamente tutti gli stakeholder chiave. Solo con il coinvolgimento degli stakeholder chiave sarà possibile iniziare a identificare le aree più critiche per la conformità.

Ogni progetto di compliance di successo inizia dagli obiettivi di business fondamentali dell'organizzazione. Le domande chiave che i team dirigenti dovrebbero porsi sono:

Qual è l'obiettivo che l'azienda vuole raggiungere nell'immediato? E tra 5-10 anni?

Quali dati (personali) sono necessari per raggiungere questi obiettivi di business strategici?

Un progetto di conformità, per quanto ben gestito, non può generare risultati ottimali se non è basato su una chiara strategia di business.

COME STRUTTURARE IL LAVORO PREPARATORIO

2. Eseguire il rilevamento e l'analisi delle lacune

Occorre quindi documentare quali dati personali sono in possesso dell'azienda, da dove provengono e con chi vengono condivisi. È importante identificare e classificare tutti i dati personali che l'azienda raccoglie, tratta e archivia. Una volta chiarito quali dati personali vengono trattati, dove, da chi e in che modo, il passo successivo consiste nell'identificare il grado di completezza delle misure di conformità attuali. Anche questa analisi delle lacune dovrebbe iniziare dalla visione strategica dei dati personali.

COME STRUTTURARE
IL LAVORO PREPARATORIO

3. Valutare i rischi

In base alle informazioni raccolte sulle attuali attività di trattamento dei dati e sulle misure di conformità corrispondenti, puoi eseguire un'analisi delle lacune per identificare le azioni necessarie per rispettare il GDPR a maggio 2018 e negli anni a seguire.

4. Creare una roadmap

Dopo avere delineato le ambizioni di business e lo stato attuale della privacy dei dati, confronta i dati emersi con i requisiti del GDPR per identificare le lacune ad alto rischio che devono essere colmate immediatamente e, in generale, definisci le priorità di conformità. Il piano d'azione dovrebbe includere tutte le attività da completare entro maggio 2018, ma anche tutte le altre azioni necessarie per assicurare la conformità a lungo termine.

5. Agire

Per una corretta esecuzione di una roadmap per il GDPR è necessario il contributo di team diversi. Nel prossimo capitolo illustreremo i ruoli di ogni funzione aziendale nella creazione di una conformità a lungo termine al GDPR.

03 CHI DEVE ESSERE COINVOLTO

Spesso la responsabilità principale del progetto preparatorio in vista del GDPR ricade su figure come il Chief Privacy Officer, il Chief Information Officer, il responsabile della conformità, il Chief Information Security Officer o simili. La scelta della persona che guiderà un progetto GDPR dipende anche dall'approccio dell'azienda al GDPR e dai requisiti specifici del settore di riferimento.

Il GDPR è una questione di rilevanza aziendale che deve coinvolgere tutti i livelli del management, dai dirigenti di alto livello alle altre cariche dell'organizzazione. È infatti fondamentale attivare una collaborazione inter-funzionale se le aziende vogliono adeguarsi ai cambiamenti normativi entro il 25 maggio 2018 e attuare una trasformazione efficace a lungo termine all'interno delle organizzazioni.

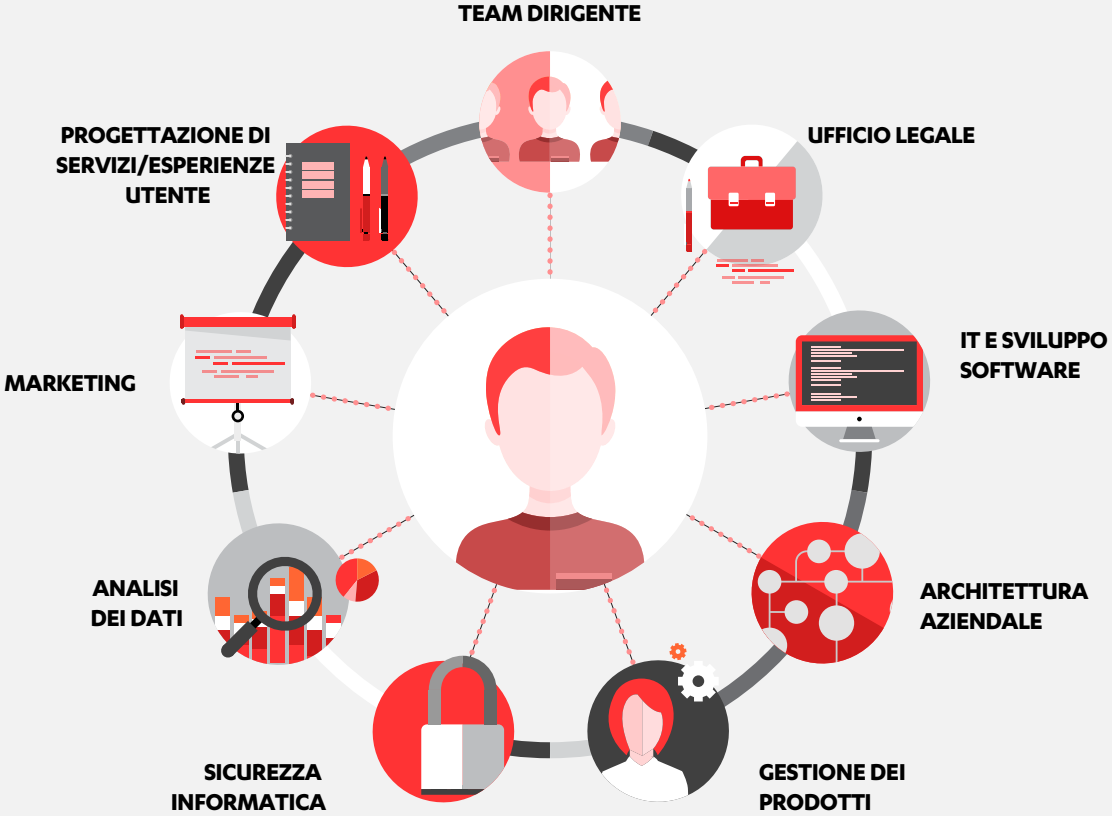
Le società che possiedono e sfruttano i dati personali di cittadini dell'UE devono coinvolgere nel processo la maggior parte dei reparti, se non tutti, e porre alcune domande basilari su come e perché i dati personali vengono raccolti e utilizzati, concentrandosi anche sul valore che hanno per le rispettive funzioni di business. Un approccio di questo tipo consentirà lo sviluppo di un business case per i cambiamenti a venire e motiverà ogni reparto ad allocare le risorse necessarie per il progetto.

La preparazione al GDPR non è solo un progetto IT, e neanche un'iniziativa che incide unicamente sul lavoro dei responsabili della privacy o della sicurezza. Tutt'altro. La collaborazione sarà un elemento cardine per la compliance. Ad esempio, gli operatori di marketing dovranno lavorare fianco a fianco con gli uffici legali e i reparti IT per gestire con trasparenza i dati personali dei clienti e i team IT devono collaborare con l'ufficio legale per rivedere gli accordi nella supply chain, modificando i contratti laddove necessario.

La combinazione degli sforzi di diverse funzioni nel lavoro preparatorio per il GDPR ha lo scopo di:

- Implementare policy, processi e procedure di conformità al GDPR nell'intera organizzazione
- Assicurare che le soluzioni IT supportino gli obiettivi di business
- Garantire che i principi di privacy by design e privacy by default vengano applicati su tutti i fronti
- Sensibilizzare l'intera azienda
- Coordinare le attività legate alla privacy dei dati in tutte le business unit

CHI DEVE ESSERE COINVOLTO



CHI DEVE ESSERE COINVOLTO

Team dirigente

Il sostegno e la collaborazione del gruppo dirigente è il primo passo per applicare il GDPR. È fondamentale avere il supporto dei dirigenti fin dall'inizio, nonché nominare un leader esecutivo per le attività di conformità. Il GDPR non è principalmente un problema di sicurezza, né riguarda solo l'IT. È un problema di rilevanza aziendale, che impone la collaborazione di tutti gli stakeholder in reparti diversi. Nominare un leader GDPR forte a livello centrale con un team GDPR principale in diverse business unit è il primo passo verso la conformità al GDPR. Il team di progetto GDPR principale deve essere responsabile nei confronti del consiglio di amministrazione e dei team dirigenti e ricevere istruzioni dall'alto.

In definitiva questo significa che la responsabilità per l'implementazione e il rispetto del GDPR dovrà essere assunta da tutta la dirigenza aziendale. Non basterà nominare un Chief Privacy Officer e lasciare a lui o a lei il compito di gestire le modifiche necessarie senza supporto e budget. Occorrerà invece una nuova mentalità aziendale, che supporti e promuova la protezione dati, non solo perché è obbligatorio, ma perché è la cosa giusta da fare per i clienti.

CHI DEVE ESSERE COINVOLTO

Ufficio legale

Il team legale di un'organizzazione dovrà conoscere a memoria il GDPR ed essere pronto a fornire consulenza al resto dell'azienda durante l'intero processo preparatorio.

È diffusa l'errata convinzione che il GDPR vieti alle aziende di utilizzare i dati personali a proprio vantaggio. Non è affatto così. Nella maggior parte dei casi è ancora possibile utilizzare dati personali a vantaggio del business, ma le organizzazioni dovranno ripensare il motivo e il modo in cui li gestiscono. Raccogliere i dati significa esserne responsabili. Ad esempio, le aziende devono informare gli interessati circa la portata delle loro attività di raccolta.

Oltre alla consulenza strategica, il team legale sarà coinvolto nelle attività pratiche di compliance, ad esempio nella revisione degli accordi legali con terze parti, soprattutto se l'azienda ha relazioni titolare-responsabile del trattamento. Tutti questi aspetti devono essere rivisti nel contesto di un programma di preparazione al GDPR.

CHI DEVE ESSERE COINVOLTO

IT e sviluppo software

La protezione dei dati non è una responsabilità esclusiva del reparto IT, ma il contributo di quest'ultimo sarà naturalmente fondamentale per il successo dell'implementazione del GDPR. I team IT sono incaricati, ad esempio, dei controlli di accesso ai dati personali e di "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento".

Il GDPR ha effetto anche sul ciclo di vita dello sviluppo software (SDLC, Software Development Life Cycle) per qualsiasi sistema che elabori i dati personali dei residenti nell'Unione Europea. Possono esservi nuovi requisiti funzionali, in particolare sui diritti di accesso degli interessati, e ovviamente è necessario garantire la sicurezza del software. Le organizzazioni devono anche raccogliere le prove delle attività legate alla privacy e alla sicurezza nel ciclo SDLC.

I proprietari dei vari sistemi IT devono conformarsi ai requisiti del GDPR dal punto di vista tecnico. Se un sistema IT ha diversi clienti interni, è necessario che i loro requisiti di sistema potenzialmente sovrapposti ma divergenti siano soddisfatti.

CHI DEVE ESSERE COINVOLTO

Architettura aziendale

Generalmente un programma GDPR è guidato dall'ufficio legale, dal reparto sicurezza informatica e dal reparto IT, ma per garantire il successo di un progetto di adeguamento al GDPR è necessario coinvolgere anche le funzioni architetturali dell'azienda. Una conformità al GDPR che sia duratura ed economica può essere raggiunta solo se l'architettura aziendale dell'organizzazione supporta i requisiti del GDPR.

Per garantire la conformità dell'organizzazione, occorre un'ampia visibilità su come vengono utilizzati i personali e perché sono stati raccolti, come vengono trattati, chi può accedervi, dove vengono archiviati, quali terze parti sono coinvolte, quali minacce interne ed esterne esistono e così via. Gli architetti aziendali hanno una visione integrata e ampia della propria organizzazione e hanno a disposizione i modelli e gli strumenti adatti per valutare, migliorare e garantire la protezione dei dati.

1. Gli architetti aziendali possono fornire informazioni approfondite su tutti i processi, le applicazioni e i dati rilevanti per la conformità al GDPR. Inoltre, possono offrire informazioni sui data object, sui flussi di dati e sulle responsabilità associate.
2. Gli architetti aziendali possono attirare l'attenzione sui rischi e sulle possibili violazioni della conformità. Possono anche aiutare i proprietari delle tecnologie a identificare i rischi tecnologici e a predisporre le misure preventive nell'ambito delle proprie responsabilità. Il ruolo degli architetti nell'identificazione dei rischi è particolarmente importante per la valutazione d'impatto.
3. Il GDPR, inoltre, non si limita a richiedere la conformità, ma impone di dimostrarla. L'architettura e i modelli architetturali costituiscono le fonti principali di queste informazioni, soprattutto quando è necessaria una visione coerente e connessa di tutto ciò che riguarda i dati personali.
4. Gli architetti aziendali possono essere fondamentali anche per definire linee guida per lo sviluppo di applicazioni che siano conformi ai nuovi principi della protezione dei dati. Queste linee guida saranno valide naturalmente per gli sviluppatori, ma anche per gli architetti di sistemi, gli architetti di database, gli analisti della sicurezza e altri dipendenti che devono essere informati circa i vari effetti del GDPR sui loro ruoli.
5. Infine, gli architetti aziendali sono nella posizione giusta per assicurare la conformità continua al GDPR e quindi svolgono un ruolo quotidiano fondamentale all'interno dei processi su cui incide il regolamento.

La conformità a lungo termine al GDPR può essere ottenuta in modo economicamente vantaggioso se l'architettura aziendale dell'organizzazione supporta i requisiti specifici del GDPR. Perché questo accada, è necessario che gli architetti dell'organizzazione siano coinvolti in modo consistente in un programma GDPR, non solo come "parti informate" ma come partecipanti attivi.

CHI DEVE ESSERE COINVOLTO

Gestione dei prodotti

I proprietari dei prodotti sono analoghi ai proprietari dei sistemi IT, ma operano nelle società di sviluppo software. Devono bilanciare lo sviluppo di funzionalità con altri requisiti, come la sicurezza e la privacy, e sono le persone chiamate a mettere in pratica i principi di "privacy by design" e "privacy by default". Il personale addetto alla gestione dei prodotti diventa sempre più rilevante quando la conformità al GDPR viene proiettata su una prospettiva a lungo termine.

Progettazione di servizi/esperienze utente

Il GDPR prevede alcuni requisiti specifici da tenere in considerazione lungo il customer journey all'interno di un servizio, per quanto riguarda le informazioni da fornire ai clienti e l'acquisizione del loro consenso. È importante valutare come è possibile integrare le nuove misure di protezione nell'esperienza del servizio senza perdere la fiducia dei clienti.

CHI DEVE ESSERE COINVOLTO

Analisi dei dati

I requisiti del GDPR in merito al ciclo di vita dei dati, soprattutto quelli relativi all'anonimizzazione e all'eliminazione dei dati, rappresentano una sfida importante per le tecnologie big data e analytics dal punto di vista dell'implementazione pratica. Occorrerà fare molto di più mediante l'anonimizzazione dei dati prima di poterli analizzare. Con il GDPR, tutti gli identificatori univoci, che siano nomi o pseudonimi, sono inclusi per legge e quindi soggetti agli stessi livelli di protezione.

È bene ribadire che non tutti i Big Data sono dati personali e spesso è possibile acquisire dati personali e anonimizzarli a scopo di analisi, estraendoli quindi dall'ambito di applicazione delle normative sulla protezione dei dati. A parte questo, l'analisi dei Big Data coinvolge nella maggior parte dei casi dati personali e quindi la protezione dei dati è assolutamente pertinente. L'Information Commissioner's Office (ICO) del Regno Unito indica tre aspetti principali da tenere in considerazione:

1. Il modo in cui i dati delle persone vengono utilizzati risulta invadente nei loro confronti? La preoccupazione principale in questo caso riguarda il possibile utilizzo dei dati per attività di profilazione degli utenti.
2. L'uso dei dati delle persone per attività di analisi dei Big Data rientra in un ambito ragionevolmente prevedibile dagli interessati?
3. Quale livello di trasparenza può avere l'azienda in merito al modo in cui tratta i dati personali? Data la complessità di gran parte delle analisi dei Big Data, questo può rappresentare una sfida.

CHI DEVE ESSERE COINVOLTO

Marketing

Il GDPR porta con sé molti cambiamenti che riguardano le attività di marketing delle organizzazioni, soprattutto nel campo del marketing digitale.

Sarà necessario rivedere e aggiornare le informative sulla privacy dei siti Web. Le aziende devono anche fare in modo che la gestione dei consensi sia adeguata e funzionante in tutti i mercati. Per quanto riguarda l'automazione del marketing e il CRM, le organizzazioni devono assicurarsi che i fornitori di strumenti e servizi siano conformi al GDPR e abbiano i diritti di utilizzo dei dati. Per ottenere tutto questo, le aziende devono formare i dipendenti e sensibilizzarli circa le implicazioni che il GDPR avrà sulle loro attività, soprattutto nel caso delle organizzazioni con team di marketing globali.

Affinché il "consenso" costituisca un fondamento di liceità per il trattamento dei dati personali, deve essere "espresso mediante un chiaro atto positivo con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano".

Il GDPR specifica precisi requisiti per il consenso di marketing. Ad esempio, quando un consenso di marketing viene revocato, le attività di marketing devono cessare immediatamente. Questo può causare difficoltà, se i dati di marketing sono stati condivisi con agenzie in formati come i fogli di Excel manuali.

Oltre al GDPR, anche la direttiva ePrivacy regola questo settore in modo rigoroso. È quindi necessario che i responsabili di marketing prestino attenzione al futuro regolamento ePrivacy, perché potrebbe incidere sulle regole di rilascio/revoca del consenso e sulle pratiche per i cookie.

CHI DEVE ESSERE COINVOLTO

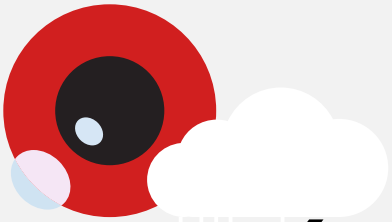
Sicurezza informatica

Il responsabile della sicurezza IT ha chiaramente uno dei ruoli più importanti nella preparazione in vista del GDPR. Il Chief Information Security Officer (CISO) è il decision maker di massimo livello per la cyber security e ha una funzione cardine nella protezione dell'azienda dagli attacchi che comportano perdite di dati. Il CISO e l'intero team di Information Security dovrebbero essere coinvolti profondamente nella definizione dei piani GDPR, data la loro centralità in alcune delle modifiche normative in materia di violazione dei dati e privacy dei dati.

Chiunque lavori nella sicurezza IT deve adoperarsi in alcune aree generali nella fase preparatoria al GDPR:

1. **Comprendere i rischi:** i team di sicurezza IT dovranno comprendere esattamente quali dati personali sui cittadini UE vengono raccolti dall'azienda e se l'esposizione di quei dati può ricadere nella definizione di violazione dei dati personali fornita dal GDPR.
2. **Prevenire le violazioni:** in questo modo, le aziende sono in grado di minimizzare il rischio di una violazione dei dati attuando misure di protezione tali da rendere più difficile un eventuale attacco.
3. **Rilevare le violazioni e rispondere rapidamente:** il nuovo obbligo di notifica entro 72 ore impone ai team di sicurezza di prepararsi a reagire a una violazione con estrema rapidità.
4. **Guardare oltre il GDPR:** ci sono molti altri aspetti dei rischi per la cyber security di cui i team di sicurezza devono occuparsi, anche se non sono indicati espressamente nel GDPR. La cyber security è un processo continuo e il miglioramento costante è l'unico modo per restare al passo.

Nella prossima sezione approfondiremo gli effetti del GDPR sulla cyber security.



04 PERCHÉ LA CYBER SECURITY È IMPORTANTE

Dal punto di vista del GDPR, i titolari del trattamento sono tenuti a stabilire se le proprie attività di trattamento, e i potenziali rischi per gli interessati che ne conseguono, sono coperti dalle misure di sicurezza attualmente implementate. A questo riguardo il regolamento non specifica le misure di sicurezza (o gli standard tecnici minimi di tali misure di sicurezza) che le aziende devono applicare per essere considerate conformi alla normativa in vigore. Il regolamento si limita a stabilire l'obbligo per le aziende di valutare e decidere quali tipi di misure devono essere implementate per rispettare le prescrizioni del GDPR e di assicurarsi che vengano adottate tutte le precauzioni necessarie per minimizzare il rischio di violazioni e fughe di dati.

La maggior parte delle organizzazioni ha implementato misure tecniche complete in tema di cyber security e protezione dei dati. Eppure, ogni mese vengono segnalate violazioni dei dati a danno di milioni di utenti. Le violazioni si susseguono senza sosta perché gli hacker sono diventati esperti negli attacchi mirati e nell'elusione delle difese. L'organizzazione deve operare basandosi sul presupposto che l'infrastruttura IT sia costantemente sotto attacco e che potenzialmente sia già stata compromessa in diversi modi. Si tratta di un cambio di prospettiva, dalla prevenzione delle minacce alla rilevazione e risposta.

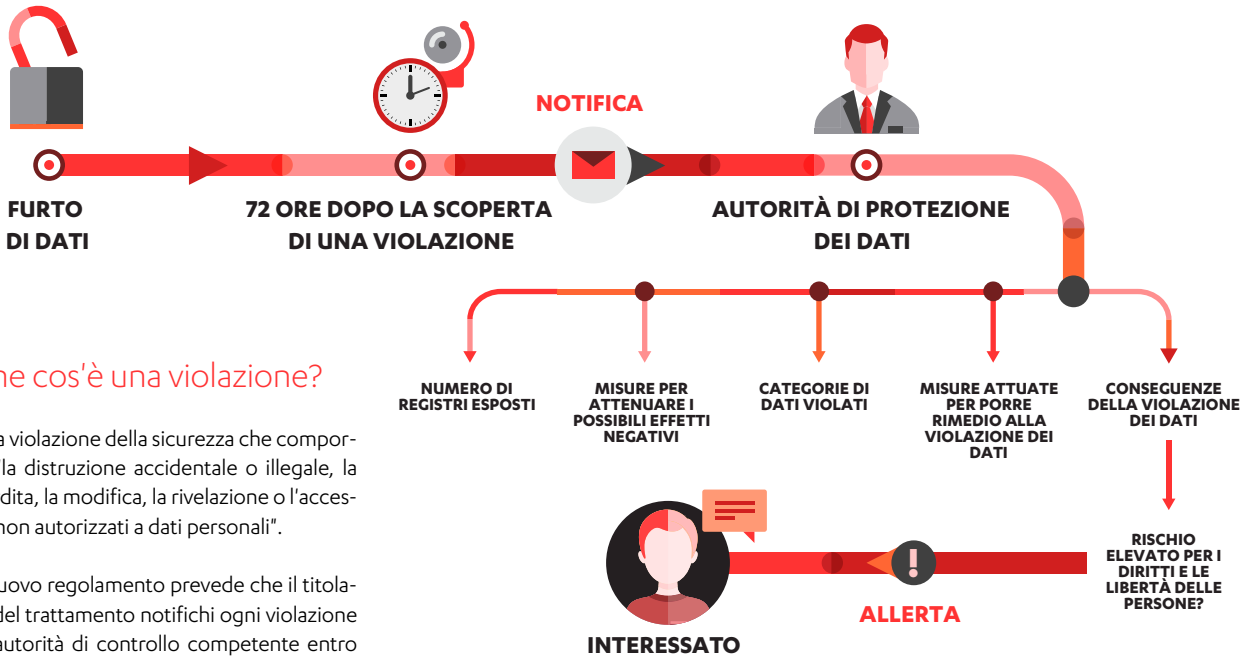
Il GDPR prevede l'obbligo di notificare la violazione dei dati personali all'autorità di controllo competente entro 72 ore dall'identificazione. Questo nuovo requisito può sovvertire le regole del gioco. In base al GDPR, le aziende dovranno fornire informazioni dettagliate su una violazione, tra cui:

1. Natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione
2. Nome e informazioni di contatto del responsabile della protezione dei dati o di altro riferimento presso cui ottenere più informazioni
3. Probabili conseguenze della violazione dei dati personali
4. Misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche per attenuarne i possibili effetti negativi

Tutto questo entro appena 72 ore. È pertanto necessario che le organizzazioni si dotino di soluzioni tecnologiche in grado di fornire visibilità sull'intera rete, in modo da rilevare e identificare la portata di una compromissione e consentire una risposta rapida ed efficace. Le soluzioni con analisi comportamentale, intelligenza artificiale e machine learning permetteranno all'azienda di scovare le minacce che sono già penetrate all'interno dei suoi confini. Se non rilevati, questi exploit possono compromettere l'infrastruttura e la proprietà intellettuale e generare i tipi di violazione dei dati previsti dal GDPR.

Cosa si evince da tutto questo? È essenziale che le aziende continuino a investire nella previsione e prevenzione delle minacce, concentrandosi anche sull'acquisizione di capacità avanzate di rilevamento degli incidenti e risposta 24/7.

PERCHÉ LA CYBER SECURITY È IMPORTANTE



Che cos'è una violazione?

Una violazione della sicurezza che comporta "la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali".

Il nuovo regolamento prevede che il titolare del trattamento notifichi ogni violazione all'autorità di controllo competente entro 24 ore dall'individuazione.

PERCHÉ LA CYBER SECURITY È IMPORTANTE

Dai dati dei clienti tratti dalle valutazioni di gestione del rischio di F-Secure emerge che la maggior parte delle grandi imprese è poco preparata ad affrontare le violazioni. Mentre il 50% dispone di un team di gestione delle crisi preparato per affrontare disastri fisici o interruzioni di attività, solo il 20% è in grado di offrire una guida efficace durante una crisi informatica. Il 65% non ha mai condotto un'esercitazione di gestione di una crisi per prepararsi a un incidente informatico.

Dotandosi delle persone, dei processi e dei controlli tecnologici appropriati, è possibile proteggere l'azienda al meglio da violazioni dei dati accidentali o dolose. L'implementazione di una roadmap di correzione e la protezione di tutti i dati personali consentono di ridurre le probabilità e i potenziali effetti negativi di una violazione dei dati.

Questi impatti, nel peggiore dei casi, possono anche essere sostanziali, il che indica anche un livello di rischio elevato. Si consideri ad esempio il rischio di una violazione dei dati rispetto al rischio rappresentato dalla mancata conformità in termini di accesso del soggetto. C'è una differenza enorme perché in una violazione dei dati si perde completamente il controllo.

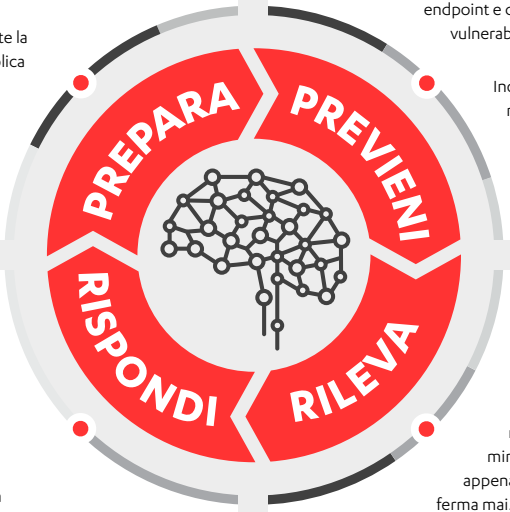
Molti articoli riguardanti il GDPR sottolineano le sanzioni pecuniarie associate al GDPR, che possono arrivare fino a 20 milioni di euro o, per le imprese, al 4% del fatturato annuo globale. Le sanzioni, in realtà, rappresentano solo una minima parte dei costi totali di una violazione dei dati. E soprattutto, le violazioni dei dati solitamente hanno conseguenze di ampia portata sotto forma di contrazione del fatturato, danno di immagine, riduzione della produttività e così via. Per questo motivo è imprescindibile investire in una soluzione adeguata per la prevenzione, il rilevamento e la risposta alle violazioni.

PERCHÉ LA CYBER SECURITY È IMPORTANTE

Scopri dove avviene il trattamento dei dati personali, qual è il ciclo di vita dei dati dalla raccolta all'eliminazione e come vengono protetti i dati in ogni fase del ciclo di vita.

Riduci l'esposizione implementando tecnicamente la minimizzazione e l'anonimizzazione dei dati. Applica la segmentazione agli asset dei dati personali e riduci la diffusione dei dati personali nei sistemi.

Crea processi e metodi di lavoro, ad esempio un piano interno di notifica e azione in caso di violazione.



Assicurati di avere applicato le misure preventive necessarie nei sistemi. Questo include, ad esempio, la protezione adeguata degli endpoint e dei servizi, nonché soluzioni di gestione delle vulnerabilità.

Inoltre, la cyber security deve essere integrata nello sviluppo dei prodotti e servizi e dei processi di acquisto fin dall'inizio, non a posteriori.

Assicurati che le persone chiave nell'organizzazione siano pronte a rispondere alle violazioni e sappiano cosa fare per contenere i danni.

Dopo un incidente, analizzalo a fondo e impara la lezione per il futuro.

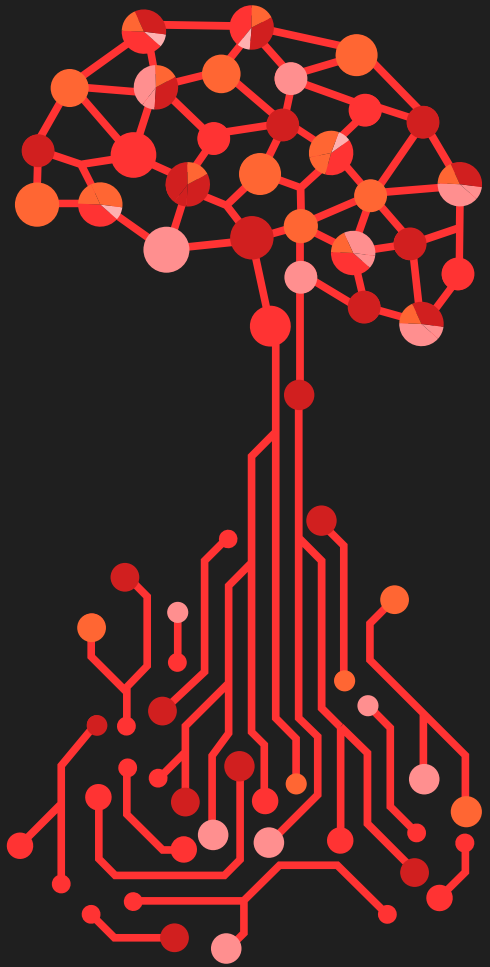
Assicurati di avere gli strumenti e soprattutto le competenze professionali necessarie per riconoscere gli incidenti e le minacce, isolarli e contenerne la diffusione non appena si verificano 24/7. La cyber security non si ferma mai.

LIVE SECURITY:
UN APPROCCIO IN COSTANTE MIGLIORAMENTO

La cyber security si muove ad altissima velocità. La superficie di attacco si espande e gli hacker sviluppano costantemente nuove tattiche per violare le difese. Nella cyber security c'è un'unica costante: il cambiamento.

Cyber security significa essenzialmente prevedere e prevenire le violazioni, rilevare quelle che si verificano e reagire in modo intelligente per minimizzarne l'impatto. Tutto questo richiede una combinazione di competenza umana e scalabilità software. Non è infatti possibile migliorare le attività di cyber security senza i migliori talenti nel campo. E non è possibile migliorare le loro conoscenze senza una tecnologia intelligente.

Dietro ogni attacco c'è una persona. E queste persone sferrano attacchi sempre più sofisticati in grado di bypassare le soluzioni puramente automatizzate. È per questo che anche alla base della difesa ci devono essere delle persone. Persone in grado di pensare come farebbe un hacker, reagire alle situazioni come la tecnologia non sa fare e istruire la tecnologia automatizzata per farla diventare sempre più intelligente giorno dopo giorno.



INFORMAZIONI SU F-SECURE

Per troppe aziende, troppi produttori e troppe persone la sicurezza è un concetto valutato a posteriori. A cosa serve essere connessi a tutto se i nostri dati, le nostre identità e le nostre transazioni non sono al sicuro?

Forti della nostra esperienza trentennale nella protezione di milioni di computer in tutto il mondo, noi abbiamo una certezza: sarai oggetto di un attacco. L'unico dubbio è se la tua azienda ha le capacità necessarie per prevedere e prevenire l'accesso ai tuoi sistemi da parte degli hacker, rilevarlo in tempo e rispondere in modo rapido ed efficace.

Per fare tutto questo, devi avere al tuo fianco il team giusto. Per F-Secure, la cyber security è ben più che un prodotto: è una visione del mondo. Leggi il nostro blog per ottenere le informazioni più recenti dal fronte del settore. E se cerchi un partner per la cyber security che ti faccia rimanere sempre un passo avanti, parliamone.

www.f-secure.com
it.safeandsavvy.f-secure.com
www.twitter.com/fsecure_it
www.facebook.com/f-secure

F-Secure