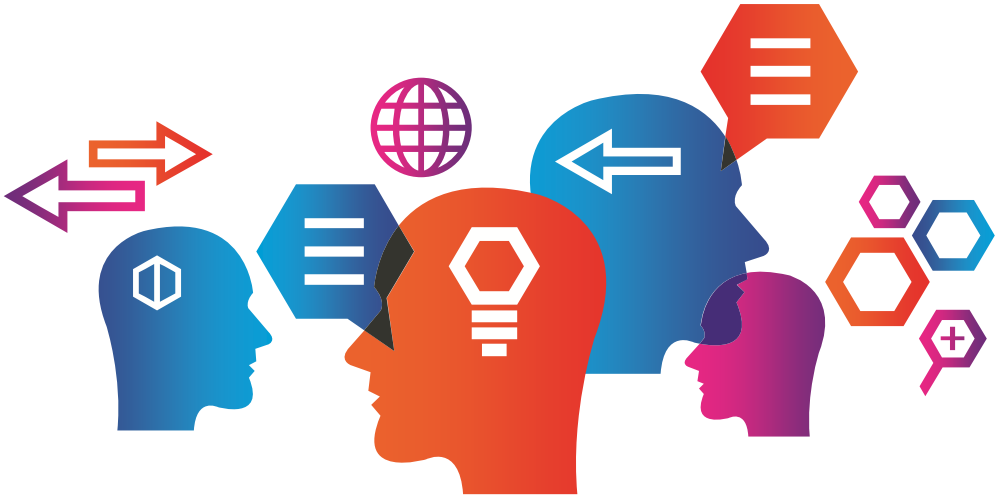


GDPR : Alcune informazioni

Il GDPR è il regolamento generale per il trattamento dei dati personali.

Che cos'è GDPR?

Cosa significa GDPR: (**General Data Protection Regulation**) è il regolamento europeo sulla protezione dei dati generali e si basa su due principi chiave.

Dare ai cittadini e ai residenti un maggiore controllo dei propri dati personali

Semplificare le normative per le imprese internazionali con una normativa unificante che si trova in tutta l'Unione Europea (UE) .

È importante tenere presente che il GDPR si applicherà a qualsiasi azienda che elabora i dati personali dei cittadini dell'UE, il che significa che potrebbe applicarsi anche a società con sede al di fuori dell'UE.

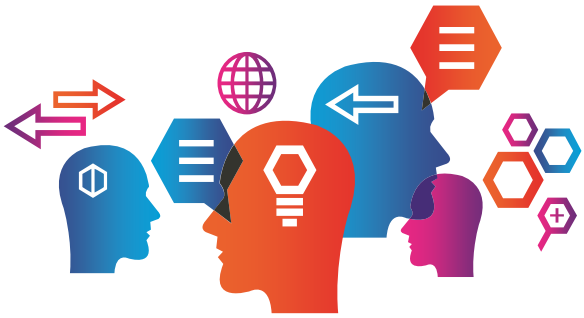
Panoramica GDPR

Le imprese le cui attività comportano il monitoraggio regolare o sistematico degli interessati su larga scala (in altre parole l'elaborazione di ampie informazioni personali) o che comportano l'elaborazione di grandi volumi di 'dati di categorie speciali', devono impiegare un responsabile della protezione dei dati (DPO). Il loro ruolo sarà quello di assicurare che la società rispetti gli obblighi previsti dal GDPR.

Il GDPR si applicherà a qualsiasi azienda che elabora i dati personali dei cittadini dell'UE, inclusi quelli con meno di 250 dipendenti (contrariamente a un comune malinteso). Gravi violazioni (ovvero qualsiasi violazione che abbia un impatto sui diritti degli interessati), devono essere segnalate immediatamente all'autorità di regolamentazione .

Questo dovrebbe avvenire entro 24 ore, ove possibile, ma almeno entro 72 ore .

La mancata conformità comporterà sanzioni fino al 4 % del fatturato annuo con massimo di 20 milioni di euro per le grandi multinazionali .



Lista di controllo GDPR per le piccole imprese

Ricorda che la tua lista di controllo deve tenere conto dei dipendenti e dei fornitori passati e presenti, nonché dei clienti (e dei dati di qualcun altro che stai ricevendo, conservando e utilizzando).

Conosci i tuoi dati?. Dovrai dimostrare di comprendere i tipi di dati personali (ad esempio nome, indirizzo, e-mail, coordinate bancarie, foto, indirizzi IP) e i dati sensibili (o di categoria speciale) (ad esempio i dettagli sulla salute o le opinioni religiose) in tuo possesso , da dove vengono, dove stanno andando e come stai usando quei dati. Identificare se si sta facendo affidamento sul consenso per l'elaborazione dei dati personali. Se lo sei (ad esempio, come parte del tuo marketing), queste attività diventeranno più difficili con il GDPR perché il consenso deve essere chiaro, specifico ed esplicito. Per questo motivo, dovresti evitare di fare affidamento sul consenso a meno che non sia assolutamente necessario.

Guarda attentamente le tue misure e le tue politiche di sicurezza. Dovrai aggiornarli per essere conformi a GDPR e, se al momento non ne hai nessuno, metterli a posto. Un ampio uso della crittografia potrebbe essere un buon modo per ridurre la probabilità di una grossa sanzione in caso di violazione.

Prepararsi a soddisfare le richieste di accesso entro un periodo di un mese. I diritti di accesso ai soggetti stanno cambiando e, in base al GDPR, i cittadini hanno il diritto di accedere a tutti i loro dati personali, rettificare qualsiasi cosa che sia inaccurata e obiettare al trattamento in determinate circostanze, o cancellare completamente tutti i dati personali che possiedi. Ogni richiesta ha un termine e una scadenza di un mese (che può essere estesa solo in circostanze attenuanti), dalla data originale della richiesta.

Allena i tuoi dipendenti e segnala una grave violazione entro 72 ore. Assicurati che i tuoi dipendenti capiscano cosa costituisce una violazione dei dati personali e costruisci processi per raccogliere eventuali “bandiere rosse”. È inoltre importante che tutti coloro che sono coinvolti nella tua attività siano consapevoli della necessità di segnalare eventuali errori al responsabile della protezione dei dati o alla persona o al team responsabile della conformità alla protezione dei dati, in quanto questa è la causa più comune di violazione dei dati.

Condurre la dovuta diligenza nella catena di fornitura. È necessario assicurarsi che tutti i fornitori e gli appaltatori siano conformi al GDPR per evitare di essere influenzati da eventuali violazioni e conseguenti sanzioni. Dovrai anche assicurarti di avere i termini contrattuali corretti con i fornitori (che impongono loro importanti obblighi, come la necessità di avvisarti tempestivamente in caso di violazione dei dati). Vedi 'Come posso controllare che i miei fornitori siano conformi al GDPR?'.

Decidere se è necessario assumere un responsabile della protezione dei dati (DPO). La maggior parte delle piccole imprese sarà esentata. Tuttavia, se le attività principali della tua azienda comportano il monitoraggio regolare o sistematico degli interessati su larga scala o che comportano l'elaborazione di grandi volumi di 'dati di categorie speciali' (dati sensibili') devi utilizzare un dato Responsabile della protezione (DPO).

Che cosa costituisce l'elaborazione dei dati 'su larga scala'?

Il GDPR non definisce ancora completamente ciò che costituisce 'su larga scala', ma alcuni esempi includono il trattamento dei dati dei pazienti da parte di ospedali, dati di viaggio e servizi di trasporto e dati dei clienti da una compagnia assicurativa o da una banca.

Appeso ai vecchi dati?

Uno dei principi chiave di GDPR è quello di richiedere alle aziende di non conservare i dati personali per un periodo di tempo più lungo del necessario o di elaborarli per scopi di cui l'individuo non è a conoscenza.
Identificare le categorie di dati - quali dati personali hai e perché - sarà molto utile per assicurarti di essere conforme al GDPR.

In che modo il GDPR definisce il 'consenso'?

Il cliente o il 'consenso' individuale è stato ridefinito e, di conseguenza, diventa molto più stretto.
Inoltre, le richieste di consenso non possono più essere nascoste in caratteri piccoli ma devono essere presentate in modo chiaro e separatamente rispetto ad altre politiche sul tuo sito Web o comunicazioni, quindi non più caselle pre-selezionate.

Note sul trattamento corretto

Può sembrare complicato, ma un avviso di trattamento equo è fornire informazioni chiare su ciò che stai facendo con i loro dati personali.

La tua nota di elaborazione corretta dovrebbe descrivere:

- perché stai elaborando i loro dati personali (lo scopo), inclusa la base legale che hai, come il consenso (consulta la pagina delle note sulla privacy per maggiori informazioni)
- le categorie di destinatari a cui inviare i dati personali (cliente, dipendente, fornitore, ecc.)
- per quanto tempo manterrai i dati (il 'periodo di conservazione') oi criteri utilizzati per determinare questi periodi di tempo
- Dovrai inoltre informare le persone dell'esistenza dei loro diritti sui dati personali

Il GDPR è così complicato - perché dovrei preoccuparmi?

È facile per le piccole aziende con una serie di cose da fare vedere il GDPR come un peso.
Ma in realtà, è qualcosa che può essere utilizzato a tuo vantaggio, aggiungendo valore alla tua attività.

Dimostrando ai potenziali ed esistenti clienti che la tua organizzazione è conforme alle nuove leggi che proteggono i diritti dei cittadini proprio come te (e i tuoi clienti), potresti portare più affari.

A nessuno piace che i propri dati vengano persi, rubati, danneggiati, utilizzati in modo improprio o condivisi senza il dovuto consenso, e fare tutto il possibile per proteggere i clienti e far crescere la loro fiducia potrebbe essere un punto di forza unico.

Quindi, dalle multe alle richieste di risarcimento, ci sono senz'altro motivi seri per ottenere la conformità a GDPR. Ma a livello di mondo reale, considera che vale la pena di organizzarti dietro le quinte, guadagnare la fiducia dei tuoi clienti ed essere la società che rispetta i dati personali, piuttosto che lasciarli seduti su un foglio di calcolo dimenticato da tempo.

Il GDPR si applica alla mia attività?
GDPR si applica a qualsiasi azienda che elabora i dati personali dei cittadini dell'UE.
Ciò include dati personali di clienti, fornitori, partner e dipendenti.

Quindi la prima domanda che devi porci è quanto spesso la tua azienda tratta i dati personali? Ciò include naturalmente i dati dei clienti, ma hai preso in considerazione i dati dei fornitori? Impiegati passati e presenti?
E c'è qualcos'altro che hai raccolto, che non rientra in nessuno di questi gruppi?

Se raccogli regolarmente questi dati, devi conformarti al GDPR, sia che i dati siano su un foglio di calcolo, sulla rete del tuo computer, sul tuo telefono cellulare o nel cloud.

Impiego meno di 250 persone. Cosa dovrei fare?

Essere una piccola impresa non significa che tu esca dall'ambito di GDPR, anche se non hai bisogno di impiegare un DPO.

È riconosciuto che le piccole imprese hanno meno risorse e rappresentano meno rischi per la protezione dei dati, pertanto ente verificatore potrebbe essere più favorevole in relazione a qualsiasi non conformità.

Tuttavia, vorrai comunque assicurarti di essere conforme ai principi del GDPR. Questo perché la tua azienda deve ancora rispettare se è coinvolta nell'elaborazione regolare (che include la raccolta, la memorizzazione e l'utilizzo) di dati personali.
È più semplice seguire il GDPR e ottenere la conformità, piuttosto che dedicare del tempo a capire come evitare il rispetto, soprattutto se lavori senza una guida legale.

È anche importante notare che anche se la tua azienda rientra in una delle esenzioni, se stai stipulando un contratto con una società più grande che conduce elaborazioni su larga scala potresti anche essere soggetto alla più dura conclusione del regolamento del GDPR.

A parte la legge, la gestione responsabile dei dati è un principio basilare di buona manutenzione aziendale.
Se sei un gruppo di una sola persona ma sei consapevole che i tuoi dischi sono un po 'dappertutto, hai pensato a come spiegare una violazione ai tuoi clienti fidati?

Rispettare i principi significa ora essere pronti per la legislazione, i rischi quotidiani e eventuali modifiche che potrebbero rendere le regole un po 'più severe per le piccole imprese, come il GDPR

A quali dati si applica la legislazione GDPR?

Vedrai molto sui 'dati personali', durante la lettura del GDPR. Ora ha una definizione più dettagliata e il regolamento ha chiarito che cose come un indirizzo IP (la stringa univoca di numeri che identifica ogni computer che comunica su Internet) contano come dati personali.
Ci sono molte altre cose che rientrano nella categoria dei dati personali.

Controllo rapido: concentrati sulle tue liste. Ad esempio, la tua azienda detiene i record delle risorse umane, gli elenchi dei clienti e i record dei dettagli dei contatti?
La maggior parte lo fa.
Che si tratti di tenere un foglio di calcolo dei dati di contatto dei clienti o di un sistema di acquisizione digitale automatizzato, verrà applicato il GDPR.

I tuoi dati sono 'sensibili'?

L'articolo 9 del GDPR definisce 'categorie speciali di dati personali' e ciò include dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale. Coprono anche dati genetici, dati biometrici, dati relativi alla salute e dati relativi alla vita sessuale o all'orientamento sessuale di una persona.
In generale, è necessario il consenso esplicito da parte di individui i cui dati personali di categoria speciale si desidera elaborare, sebbene l'articolo 9 preveda una serie di eccezioni a questa regola.

Il GDPR cambia la tua responsabilità

Una cosa che contraddistingue davvero il GDPR sono le modifiche apportate alla 'responsabilità' dei processori di dati.
Questo è un cambiamento rispetto a prima, che ha posto più responsabilità sul controller dei dati.
Questi sono i principi base su cui devi pensare. Non rimanere impigliato sul fatto che tu sia un controllore o un processore in quanto entrambe le parti sono obbligate ad apportare modifiche al fine di rispettare GDPR.
In questa fase, la cosa fondamentale è pensare ai dati personali che la tua piccola impresa raccoglie, detiene, usa e condivide e quanto sei sicuro che i nuovi principi siano veri.

Sono un controller di dati o un elaboratore di dati?

Il GDPR si applicherà ai 'controllori' e ai 'processori' dei dati. In generale, l'elaborazione è definita come qualsiasi operazione eseguita su dati personali, come la memorizzazione, la raccolta, la registrazione, l'organizzazione, la condivisione, la cancellazione, la consultazione, ecc. Anche un controllore è un elaboratore di dati, ma deciderà anche lo scopo dei dati e attività di elaborazione.

Ad esempio, se sei una piccola azienda che offre un servizio di idraulica e i dettagli dei tuoi clienti sono gestiti tramite un'app di gestione dei contatti sul tuo telefono, ospitata da una terza parte, questo generalmente ti rende il controller e il processore di terze parti.
Se d'altra parte, gestisci tutti i tuoi dati su un foglio di calcolo che hai creato da solo, sei sia controller che processore.

Quali sono le sanzioni del GDPR?

Il GDPR rafforza le pene già esistenti nell'ambito del DPA. Queste penalità esistenti includono:
Procedimenti penali, inclusi pene detentive per violazioni deliberate
Impegni obbligatori, in cui la tua azienda deve impegnarsi in azioni specifiche per migliorare la conformità
Con l'inizio del GDPR a maggio, queste sanzioni diventeranno più pesanti.
Le imprese in violazione vedranno un drammatico aumento delle ammende con penalità che raggiungono un limite massimo di 20 milioni di euro o il quattro per cento del fatturato globale annuo, a seconda di quale sia il più alto.

IT CONSULTING | CONSULENZA | MARKETING | SITI INTERNET | CLOUD SERVICES

www.buildingthefuture.it

INFORMATION TECHNOLOGY e CONSULENZA AZIENDALE

Tel: 0362.179.4998

gianguerrini@buildingthefuture.it

Building THE FUTURE

I nostri servizi “GDPR” pensati per le PMI

Buiding The Future S.r.l. ha pensato in questi mesi di svolgere una indagine ad ampio spettro per comprendere come poter supportare I clienti che desiderano mettersi in regola con tale normative.

La nostra società come sempre, prima di dare una proposta ai propri clienti, e ai nuovi potenziali clienti, ha cercato di pensare ad un approccio pratico e modulare, **cercando di contornarsi delle persone giuste e con le competenze adeguate per assicurare una consulenza adeguata:**

Esperto avvocato: che abbia studiato a fondo la normativa GDPR, da molto tempo e che possa in caso di caisistiche particolari dare un apporto legale alla prblematica da fforntare

Esperto sulla norma GDPR: Persona competente che può supportare il cliente nella analisi preliminare e redazione dei documenti o al quale anche demandare, se richiesto e necessario, anche l’incarico di DPO esterno.

Esperto informatico IT: che analizzerà il corretto adeguamento della infrastruttura informatica e redigerà un documento di Gap Analysis da allegare alla analisi del rischio.

Abbiamo pensato quindi a delle proposte flessibili, che si potessero adattare alla situazione reale di un cliente, che potrebbe avere esigenze diverse. Di seguito alcuni esempi:

Caso A (chiavi in mano) : il cliente sta cercando un unico interlocutore, inteso come società, alla quale affidare l’adeguamento del GDPR, affidandosi al team proposto da Building The Future.

Caso B: Il cliente ha già un proprio consulente esterno (p.e. proprio avvocato o esperto GDPR) , che si preoccuperà della gestione e creazione della documentazione per l’adeguamento al GDPR, ma ha bisogno di un consulente informatico, per la redazione del documento di analisi del rischio informatico e delle misure di adeguamento della infrastruttuttura della rete aziendale

Caso C: Viene richiesto oltre al servizio consulenza informatica IT, per la redazione del documento di analisi e adeguamento della rete aziendale, anche una proposta di fornitura , se necessaria, Hardware e attività sistemistica per applicare l’adeguamento minimo ed indispensabile per essere in regola con il GDPR.

Per chi fosse interessato preghiamo quindi di inoltare la richiesta contattandoci compilano il fomr Conatti dal nostro sito internet www.buildingthefuture.it oppure inviando una email di richiesta a gianguerrini@buildingthefuture.it .

Preghiamo di indicare nella richiesta:

Nome azienda:

Numero dipendenti:

Settore merceologico:

Telefono / Cellulare:

Quale servizio siete interessati ? : Caso A, Caso B, Caso C.