COS'È IL GDPR?

Per "**GDPR**" ("*General Data Protection Regulation*") si intende il nuovo Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali. La nuova normativa è entrata pienamente in vigore in tutti i Paesi dell'Unione Europea il **25 maggio 2018**.

Il GDPR introduce importantissime novità per cittadini e imprese, con l'obiettivo dichiarato di elevare il livello di protezione dei dati, rafforzare la fiducia dei cittadini e sostenere la crescita dell'economia digitale.

Come faccio a sapere se la mia attività deve adeguarsi al GDPR?

Se sei un'azienda o uno studio professionale che tratta dati personali in Italia o in un altro Paese dell'Unione Europea, sei tenuto ad adeguarti al GDPR. Il GDPR si applica anche a imprese ed enti che hanno sede al di fuori dell'Unione Europea, ad esempio se vendono beni o servizi, anche via internet, all'interno dell'Unione Europea.

Ma che cos'è un dato personale? In pratica, un dato personale è qualunque informazione riconducibile ad un individuo. Ad esempio, sono dati personali il nome e cognome di una persona e tutti i suoi dati anagrafici, l'indirizzo e-mail, il numero di telefono, ma anche una fotografia, i suoi dati biometrici (es. l'impronta digitale o le caratteristiche della sua firma autografa), il suono della sua voce, le sue abitudini alimentari. Alcune categorie di dati (come quelli relativi ai dati genetici, allo stato di salute, all'orientamento sessuale o all'apparenza a partiti e sindacati) sono considerati sensibili e richiedono misure aggiuntive di protezione in base alla normativa.

Quali sono le mie responsabilità come azienda o studio e cosa rischio?

Ai sensi del GDPR, dovrai adottare tutte le misure di protezione dei dati previste dalla normativa. Ecco alcuni esempi di quello che dovrai fare per adeguarti al GDPR:

- informa in modo chiaro, semplice e non "legalese" i tuoi clienti, dipendenti e gli altri interessati, di come tratti i loro dati: dì loro chi sei quando richiedi dei dati, perché li stai trattando, per quanto tempo verranno conservati e a chi devono essere comunicati;

- chiedi in modo esplicito il consenso delle persone di cui raccogli i dati; in caso di minori, verifica il limite di età per chiedere il consenso dei genitori;
- assicurati di poter rispondere alle richieste degli interessati: il GDPR attribuisce a tutte le persone il diritto di sapere chi tratta i loro dati e la motivazione. Possono inoltre richiedere la modifica e la cancellazione di tali dati. Hanno il diritto di opporsi al marketing diretto e alla profilazione, oltre che il diritto di trasferire i propri dati ad un'altra azienda (i.e. portabilità);
- in caso di violazioni di dati o *data breach* – ad esempio, in caso di divulgazione non autorizzata di dati a causa di un problema di sicurezza – dovrai darne comunicazione entro 72 ore all'Autorità di controllo;
- nel caso in cui tu intenda affidare operazioni di trattamento a fornitori o altri soggetti esterni, dovrai assicurarti di ricorrere solamente a responsabili del trattamento che presentino sufficienti garanzie in merito alla conformità al Regolamento e alla tutela dei diritti degli interessati.

Il nuovo Regolamento prevede rilevanti sanzioni in caso di violazione, che comprendono multe fino a 20 milioni di Euro o – nel caso di imprese – fino al 4% del fatturato globale dell'esercizio precedente, se superiore.

Cosa devo fare per adeguarmi e da dove cominciare?

La nuova normativa richiede di adottare una serie di misure per proteggere in modo adeguato i dati delle persone con cui la tua azienda o il tuo studio si trova ad operare, ad esempio i dati dei tuoi dipendenti e dei tuoi clienti.

La prima cosa da fare, quindi, è **prendere consapevolezza**:

- Informati (ad esempio visitando i seguenti link:
    - http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali
    - http://ec.europa.eu/justice/smedataprotect/index_it.htm
    - https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_it)

  e valuta quali tra le novità introdotte dal nuovo Regolamento sono applicabili alla tua attività.

- Attivati per capire quali dati tratta la tua azienda o il tuo studio, a chi appartengono, per quali finalità li utilizzi, a quali rischi sono esposti e a chi vengono comunicati.

- Documenta i trattamenti dei dati che hai individuato: il GDPR richiede di tenere (anche in formato elettronico) un Registro aggiornato dei dati personali che gestisci. Il Registro dei trattamenti potrebbe non essere necessario in alcuni casi specifici. Tuttavia, anche in questi casi è raccomandata la sua tenuta dal Garante per la Protezione dei dati personali, in quanto rappresenta uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte dell'Autorità di controllo, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti svolti ed è uno strumento indispensabile per ogni valutazione e analisi del rischio.

Per tenere il Registro dei trattamenti e curare gli altri adempimenti richiesti al GDPR, potrai utilizzare le nostre innovative soluzioni software che ti possono supportare in modo facile e intuitivo nella gestione delle attività di compliance.

Cosa si intende per "trattamento" di dati personali? Quali trattamenti esegue tipicamente un'azienda o uno studio professionale?

Per "trattamento" si intende qualunque tipo di operazione che viene svolta su dati personali. Ad esempio, raccogliere dei dati creando un archivio o una banca dati, creare copie dei dati, accedere ai dati in lettura o modifica, comunicare i dati a terzi e trasmetterli via internet o con altre modalità sono tutte operazioni di trattamento soggette al GDPR.

I trattamenti sono normalmente descritti – ad esempio ai fini della compilazione del Registro dei trattamenti – indicando il riferimento ai processi utilizzati o alle banche dati aziendali.

Ecco alcuni esempi di banche dati e attività la cui gestione rappresenta tipicamente un'operazione di trattamento da parte di studi professionali e aziende:

- anagrafiche clienti;
- anagrafiche dipendenti;
- anagrafiche fornitori;
- videosorveglianza;
- campagne commerciali e di marketing;
- gestione di un sito web;

Che cosa sta facendo Nextsoft Srls per il GDPR?

Nextsoft, ha avviato da tempo un progetto di adeguamento al GDPR con un team di professionisti legali ed esperti per migliorare le caratteristiche di sicurezza dei propri prodotti e servizi ed elevare il livello di protezione dei dati personali.

- Stiamo aggiornando i nostri applicativi allo scopo di introdurre funzionalità specifiche per aiutare i clienti a soddisfare i requisiti di *compliance* previsti dal GDPR, secondo le logiche della privacy by design e privacy by default richieste dal GDPR.
- Stiamo rafforzando le misure di sicurezza nei servizi erogati ai clienti allo scopo di ridurre i rischi di trattamenti non conformi, introducendo il principio della protezione dei dati personali sin dalle fasi di sviluppo e progettazione degli applicativi.

La NextSoft srls è responsabile nei confronti del cliente per come tratta i suoi dati?

Laddove la Nextsoft Srls tratta i dati personali di cui il cliente è titolare, acquista il ruolo di "Responsabile del trattamento di dati" ai sensi dell'art. 28 GDPR e, in quanto tale, è tenuta ad assicurare che i dati personali del cliente siano trattati nel rispetto delle misure di sicurezza previste dal GDPR. Per regolare gli obblighi assunti dalla nostra società come Responsabile del trattamento, abbiamo predisposto uno specifico Accordo per la Protezione dei dati personali (Data Processing Agreement o "DPA"). Esso riflette accuratamente ed in modo puntuale le misure intraprese dalla NextSoft srls per assicurare la conformità al GDPR in rapporto ai diversi servizi e prodotti erogati. Il DPA, così come le condizioni speciali di trattamento applicabili alle diverse categorie di prodotto, sono disponibili a questo link.

In cosa consiste un "Accordo per il trattamento dei dati personali"?

L'accordo per il trattamento dei dati personali (Data Processing Agreement o "DPA"), disponibile a questa pagina, descrive le condizioni e le modalità di trattamento dei dati personali eseguito dalla Nextsoft srls, le responsabilità connesse alle attività di trattamento, ivi incluso l'impegno assunto quale Responsabile del trattamento dei dati personali ai sensi dell'art. 28 GDPR.

Le caratteristiche specifiche del trattamento dei dati personali con riguardo a ciascun prodotto e servizio sono descritte nei rispettivi "DPA - Condizioni speciali di trattamento", disponibili al medesimo link. La Nextsoft Srls ha predisposto il DPA, aggiornando le proprie condizioni contrattuali, per conformarsi agli obblighi previsti dal nuovo Regolamento Europeo e per assicurare ai propri clienti un corretto trattamento dei loro dati.

Perché devo concludere con la Nextsoft Srls un "Accordo per il trattamento dei dati personali"?

Il GDRP (art. 28, comma 3) prevede che il trattamento dei dati personali da parte di un responsabile per conto di un titolare sia regolato da un contratto o un altro atto giuridico vincolante, in cui siano definiti:

- la natura e le finalità del trattamento;
- le misure tecniche e organizzative adottate;
- i diritti e gli obblighi delle parti.

La definizione di un accordo contrattuale che regoli le attività svolte dalla nostra società come responsabile del trattamento, costituisce pertanto, adempimento di una prescrizione legale (art. 28 GDPR). Per questo motivo, abbiamo aggiornato le nostre condizioni contrattuali e predisposto uno specifico "Accordo generale per la Protezione dei dati" in modo da regolare in maniera puntuale i diritti e gli obblighi della nostra società e del cliente con riguardo particolare alla protezione dei dati personali.

Sono già un vostro cliente: devo sottoscrivere anch'io il DPA predisposto dalla Nextsoft Srls?

No, le condizioni contrattuali sono già state integrate mediante lo specifico Accordo per la Protezione dei dati personali (Data Processing Agreement o "DPA"), che riflette accuratamente ed in modo puntuale le misure intraprese per assicurare la conformità al GDPR e per regolare le attività svolte in qualità di "Responsabile del trattamento" (art. 28 GDPR).

Il DPA, consultabile al seguente link http://colibricorporation.com/gdpr costituisce quindi già parte integrante delle condizioni generali di contratto.

I miei dati sono al sicuro?

Si. I dati personali che i clienti ci affidano sono sempre trattati unicamente allo scopo di eseguire i servizi richiesti, nel rispetto delle rigorose normative in materia di protezione dei dati personali.

Come produttori di software, abbiamo costantemente rafforzato i nostri investimenti nell'implementazione di misure di sicurezza e protezione dei dati proprio per offrire ai clienti un servizio sempre più sicuro e affidabile.

Che cosa ci fate con i miei dati?

I dati personali che i clienti ci affidano sono sempre trattati unicamente allo scopo di eseguire i servizi richiesti, nel rispetto delle rigorose normative in materia di protezione dei dati personali.

Quali sono le misure adottate dalla Nextsoft Srls al fine di garantire il corretto trattamento dei dati?

Nelle operazioni di trattamento dei dati personali che Nextsoft Srls esegue per conto dei propri clienti in qualità di "Responsabile del trattamento di dati personali", adotta specifiche misure tecnico-organizzative al fine di evitare il trattamento illecito o non autorizzato, la distruzione accidentale o illecita, il danneggiamento, la perdita accidentale, l'alterazione e la divulgazione non autorizzata di dati personali. Le misure adottate da Nextsoft Srls sono descritte in modo puntuale nell'Accordo per la protezione dei dati personali o "**DPA**".