GENNAIO 2023

GDPR: gli obblighi per le imprese

LE GUIDE DELLA DIGITALIZZAZIONE - #1

A cura di

EXASYS SRL

Quello che ogni impresa deve sapere sul regolamento generale sulla protezione dei dati dell'UE

Il regolamento generale sulla protezione dei dati (GDPR) regola il modo in cui le imprese trattano e gestiscono i dati personali. In vigore dal 25 maggio 2018 e applicabile a tutte le imprese e organizzazioni (ad esempio ospedali, amministrazioni pubbliche ecc), rappresenta il più grande cambiamento alle norme dell'Unione europea (UE) in materia di protezione dei dati in oltre 20 anni.

Il regolamento non solo conferisce ai cittadini un maggiore controllo sulle modalità di utilizzo dei loro dati personali, ma semplifica notevolmente anche il contesto normativo per le imprese. Per farlo, definisce un quadro normativo uniforme per la protezione dei dati in tutta l'UE In altre parole, anziché avere leggi diverse sulla protezione dei dati in ogni paese, ora l'intera UE è disciplinata da un unico regolamento In questo modo, un'azienda che opera in paesi diversi non deve più rispettare normative varie e spesso divergenti.

Per poter offrire i suoi servizi ovunque nell'UE, dovrà semplicemente rispettare il GDPR.

I vantaggi del regolamento per la tua azienda

- Un'Unione, una legge: con un insieme unico di norme, operare nell'UE sarà più semplice per le imprese
- Uno «sportello unico»: nella maggior parte dei casi, le aziende hanno a che fare con un'unica autorità per la protezione dei dati
- Norme europee sul territorio europeo: le aziende con sede al di fuori dell'UE devono applicare le stesse norme delle aziende europee quando offrono i loro beni o servizi a persone all'interno dell'Unione europea
- Approccio basato sul rischio: il regolamento evita un obbligo oneroso e uguale per tutti
- Regole che si adattano all'innovazione: il regolamento è neutrale sotto il profilo tecnologico.

È una questione di fiducia

La protezione dei dati personali è una questione che preoccupa molto le persone. La fiducia negli strumenti digitali rimane bassa. Infatti, secondo un sondaggio Eurobarometro:

- otto persone su dieci ritengono di non avere il controllo completo dei loro dati personali;
- sei su dieci dicono di non fidarsi delle aziende online;
- oltre il 90 % degli europei dichiara di volere gli stessi diritti di protezione dei dati in tutti i paesi dell'UE.

Il regolamento generale sulla protezione dei dati rappresenta una nuova opportunità per la tua azienda di migliorare la fiducia dei consumatori attraverso una gestione dei dati personali basata sul rischio.

Il GDPR si applica alla mia impresa?

In sintesi, il regolamento generale sulla protezione dei dati si applica a tutte le imprese che trattano i dati personali mediante un trattamento automatizzato o manuale (a condizione che i dati siano organizzati in base a criteri).
Anche se la tua impresa tratta i dati solo per conto di altre aziende, dovrà comunque rispettare la legge.

Cosa sono i dati personali

I dati personali sono tutte le informazioni relative a una persona vivente identificata o identificabile, ad esempio:

- nome
- indirizzo e numero telefonico
- posizione
- dati sanitari
- dati sul reddito e bancari
- preferenze culturali
- ... ecc

I dati personali sottoposti a deidentificazione o pseudonimizzazione, ma che possono essere utilizzati per reidentificare una persona, rientrano nell'ambito di applicazione del regolamento. Invece, i dati personali resi irreversibilmente anonimi in modo tale che la persona non sia più identificabile non sono considerati dati personali e non sono perciò disciplinati dal regolamento.

Il regolamento è inoltre neutrale sotto il profilo tecnologico, vale a dire protegge i dati personali indipendentemente dalla tecnologia utilizzata o dalle modalità di conservazione dei dati personali Che la tua impresa tratti e conservi dati personali utilizzando un sofisticato sistema IT o tramite file cartacei, dovrà comunque rispettare il GDPR.

Attenzione alle categorie di dati personali speciali (sensibili)

Se i dati personali raccolti includono informazioni sulla salute, la razza, l'orientamento sessuale, la religione, le convinzioni politiche o l'appartenenza a un sindacato di una persona, sono considerati sensibili. La tua azienda può trattare questi dati solo a determinate condizioni e potrebbe essere necessario fornire ulteriori garanzie, come la crittografia.

Cosa implica il trattamento dei dati personali?

Secondo il regolamento generale sulla protezione dei dati, azioni quali la raccolta, l'utilizzo e la cancellazione dei dati personali rientrano nella definizione di trattamento dei dati personali.

Controlli i tuoi locali tramite telecamere a circuito chiuso?
Consulti una banca dati contenente dati personali per scopi commerciali?
Invii email promozionali? Cancelli file (digitali) dei dipendenti o distruggi documenti?
Pubblichi una foto di una persona sul tuo sito web o sui canali dei social media?

Se hai risposto «sì» a una qualsiasi di queste domande, allora la tua azienda tratta dati personali.

In che modo il regolamento contribuisce a ridurre i costi?

Il regolamento generale sulla protezione dei dati tiene conto delle esigenze delle imprese.
Ad esempio, esso mira a sopprimere gli obblighi amministrativi per ridurre i costi e ridurre al minimo gli oneri. Nessuna notifica preventiva: la riforma elimina la maggior parte delle notifiche preventive alle autorità di vigilanza e i relativi costi.

Il responsabile della protezione dei dati: le aziende devono nominare un responsabile della protezione dei dati se le loro attività principali prevedono il trattamento di dati sensibili su vasta scala o un monitoraggio regolare, sistematico e su vasta scala di persone.

Le pubbliche amministrazioni hanno l'obbligo di nominare un responsabile della protezione dei dati. Le aziende sono obbligate a effettuare una valutazione d'impatto sulla protezione dei dati soltanto se l'attività di trattamento dei dati proposta comporta un rischio elevato per i diritti e le libertà delle persone. Conservazione delle registrazioni: le aziende con meno di 250 dipendenti non hanno l'obbligo di tenere registri, a meno che il trattamento dei dati non sia occasionale o riguardi dati sensibili.

I tuoi obblighi ai sensi del Regolamento

Il regolamento generale sulla protezione dei dati impone obblighi diretti in materia di trattamento dei dati alle imprese a livello dell'UE. Ai sensi del regolamento, un'azienda può elaborare dati personali solo a determinate condizioni.

Ad esempio, il trattamento deve essere equo e trasparente, per uno scopo specifico e legittimo e limitato ai dati necessari per adempiere tale scopo Deve inoltre fondarsi su una delle seguenti basi giuridiche:

- il consenso della persona interessata;
- un obbligo contrattuale tra te e la persona;
- soddisfare un obbligo giuridico;
- proteggere gli interessi vitali di una persona;
- svolgere un compito di interesse pubblico;
- per i legittimi interessi della tua azienda, ma solo dopo aver verificato che non vengano compromessi i diritti e le libertà fondamentali della persona di cui stai trattando i dati.

Se i diritti della persona prevalgono sui tuoi interessi, non puoi trattare i dati.

Approfondimento: ottenere il consenso al trattamento dei dati personali

Il regolamento applica regole severe per il trattamento dei dati basato sul consenso.
Lo scopo di queste norme è di garantire che la persona capisca a cosa sta fornendo il consenso.
Ciò significa che il consenso deve essere liberamente espresso, specifico, informato e inequivocabile, mediante una richiesta presentata in un linguaggio chiaro e comprensibile. Inoltre, il consenso deve essere fornito con un atto affermativo, ad esempio spuntando una casella online o firmando un modulo.
Se tratti i dati personali relativi a un minore sulla base del consenso, è necessario il consenso dei genitori.Tuttavia, poiché la soglia di età varia dai 13 ai 16 anni tra i diversi paesi, ti consigliamo di consultare la legislazione nazionale.

Una volta stabilito che il regolamento generale sulla protezione dei dati si applica alla tua impresa e che ha luogo un trattamento di dati personali, il passo successivo è quello di determinare il tuo ruolo. Le norme in materia di protezione dei dati distinguono tra il titolare del trattamento e il responsabile del trattamento, con obblighi diversi per ciascuno di essi. Mentre il titolare del trattamento definisce le finalità e le modalità del trattamento dei dati personali, il responsabile del trattamento tratta i dati personali solo per conto del titolare del trattamento.

Questo non significa però che il responsabile possa semplicemente nascondersi dietro al titolare del trattamento.

Il regolamento richiede che il titolare del trattamento si avvalga solo di un responsabile del trattamento che offra sufficienti garanzie. Queste garanzie devono essere incluse in un contratto scritto tra il titolare e il responsabile del trattamento.

Il contratto deve contenere anche una serie di clausole obbligatorie, tra cui, ad esempio, una clausola secondo cui il responsabile del trattamento tratta i dati personali solo in base a istruzioni documentate del titolare del trattamento.

Il regolamento generale sulla protezione dei dati prevede una serie di obblighi volti a tutelare il diritto di una persona ad avere il controllo sui propri dati personali.

I tuoi obblighi: **fornire informazioni trasparenti**.

Le aziende devono fornire alle persone informazioni su chi tratta che cosa e perché. Queste informazioni devono indicare chiaramente almeno quanto segue:

- chi sei
- perché stai trattando i dati
- qual è la base giuridica
- chi riceverà i dati (se applicabile).

In alcuni casi, le informazioni devono anche indicare:

- i dati di contatto del responsabile della protezione dei dati
- l'interesse legittimo (quando l'interesse legittimo costituisce la base giuridica del trattamento)
- la base per il trasferimento dei dati verso un paese al di fuori dell'UE
- per quanto tempo saranno conservati i dati
- i diritti in materia di protezione dei dati della persona (ossia il diritto di accesso, rettifica cancellazione, limitazione, obiezione, portabilità ecc)
- le modalità di ritiro del consenso (quando il consenso costituisce la base giuridica del trattamento)
- se esiste un obbligo legale o contrattuale di fornire i dati
- nel caso di decisioni automatizzate, informazioni sulla logica, la rilevanza e le conseguenze della decisione.

I tuoi obblighi: il diritto di accesso e il diritto alla portabilità dei dati

Le persone hanno il diritto di richiedere l'accesso ai dati personali che le riguardano, gratuitamente e in un formato accessibile.
Se ricevi questo tipo di richiesta, devi:

- comunicare all'interessato se stai trattando i suoi dati personali;
- informarlo in merito al trattamento (le finalità del trattamento, le categorie di dati personali interessati, i destinatari dei suoi dati ecc);
- fornire una copia dei dati personali che stai trattando.

I dati devono essere forniti in un formato comunemente utilizzato e leggibile da un dispositivo automatico. Anche se questi due diritti sono strettamente correlati, si tratta comunque di due diritti distinti. Pertanto, devi assicurarti di non fare confusione tra i due e informare l'interessato di conseguenza.

In alcuni casi, una persona può chiedere al titolare del trattamento di cancellare i propri dati personali, ad esempio quando i dati non sono più necessari alle finalità del trattamento. La tua azienda non è però obbligata a soddisfare tale richiesta se:

- il trattamento è necessario per rispettare la libertà di espressione e di informazione;
- è necessario conservare i dati personali per adempiere un obbligo giuridico;
- ci sono altri motivi di interesse pubblico per conservare i dati personali, quali la salute pubblica o finalità di ricerca scientifica e storica;
- è necessario conservare i dati personali per l'esercizio di un diritto in sede giudiziaria.

I tuoi obblighi: il diritto di rettifica e il diritto di opposizione

Se una persona ritiene che i suoi dati personali siano errati, incompleti o inesatti, ha il diritto di farli correggere o completare senza indebito ritardo.
Una persona può anche opporsi in qualsiasi momento al trattamento dei suoi dati personali per una particolare finalità quando la tua azienda li tratta sulla base di un interesse legittimo o per lo svolgimento di un compito di interesse pubblico.
A meno che tu non abbia un interesse legittimo che prevale sull'interesse della persona, dovrai interrompere il trattamento dei dati personali.
Allo stesso modo, una persona può chiedere di limitare il trattamento dei suoi dati personali mentre si stabilisce se il tuo interesse legittimo prevalga o meno sul suo interesse. Nel caso del marketing diretto, invece, sei sempre obbligato a interrompere il trattamento dei dati personali su richiesta dell'interessato.

Le persone hanno il diritto di non essere oggetto di una decisione basata esclusivamente su un trattamento automatizzato. Vi sono tuttavia alcune eccezioni a questa regola, ad esempio quando la persona ha esplicitamente acconsentito alla decisione automatizzata Tranne nei casi in cui la decisione automatizzata è basata su una legge, la tua azienda deve:

- informare la persona in merito alla decisione automatizzata;
- garantire all'interessato il diritto di ottenere il riesame della decisione automatizzata da parte di una persona;
- dare alla persona la possibilità di contestare la decisione automatizzata.

I tuoi obblighi: nominare un responsabile della protezione dei dati

Il responsabile della protezione dei dati verifica il rispetto del regolamento da parte della tua azienda.
Uno dei compiti più importanti consiste nell'informare e fornire consulenza ai dipendenti che si occupano del trattamento dei dati personali in merito ai loro obblighi. Collabora inoltre con l'autorità per la protezione dei dati, fungendo da punto di contatto nei confronti dell'autorità e delle singole persone.

La tua azienda è tenuta a nominare un responsabile della protezione dei dati quando:

- monitora regolarmente o sistematicamente le persone o tratta categorie particolari di dati;
- il trattamento è una delle attività principali dell'azienda;
- il trattamento viene eseguito su vasta scala.

Ad esempio, se si trattano dati personali per indirizzare la pubblicità attraverso i motori di ricerca in base al comportamento online delle persone, il regolamento richiede la presenza di un responsabile della protezione dei dati. Se, invece, invii ai tuoi clienti materiale promozionale solo una volta all'anno, non avrai bisogno di un responsabile della protezione dei dati.
Allo stesso modo, se sei un medico che raccoglie dati sulla salute dei pazienti, probabilmente non è necessario un responsabile della protezione dei dati, ma sarà necessario se tratti dati personali sanitari e genetici per un ospedale.

I tuoi obblighi: la protezione dei dati fin dalla progettazione e di default

Il regolamento generale sulla protezione dei dati introduce due nuovi principi: la protezione dei dati fin dalla progettazione e la protezione dei dati di default.
La protezione dei dati fin dalla progettazione contribuisce a garantire che un'azienda tenga conto della protezione dei dati fin dalle prime fasi della pianificazione di nuove modalità di trattamento dei dati personali. In base a tale principio, il titolare del trattamento deve adottare tutte le misure tecniche e organizzative necessarie per attuare i principi di protezione dei dati e tutelare i diritti delle persone, ad esempio attraverso l'uso della pseudonimizzazione.
La protezione dei dati fin dalla progettazione riduce al minimo i rischi per la privacy e aumenta la fiducia.

I tuoi obblighi: inviare una notifica adeguata in caso di violazione dei dati

Si verifica una violazione dei dati quando i dati personali di cui sei responsabile vengono comunicati a destinatari non autorizzati, accidentalmente o illegalmente, oppure resi temporaneamente indisponibili o alterati.

Per un'impresa, è fondamentale attuare misure tecniche e organizzative adeguate per evitare una violazione dei dati. Tuttavia, se la violazione si verifica e costituisce un rischio per i diritti e le libertà individuali, è necessario informare l'autorità per la protezione dei dati competente entro 72 ore dopo aver preso conoscenza della violazione.
A seconda che la violazione dei dati costituisca o meno un rischio elevato per le persone interessate, un'azienda potrebbe anche dover informare tutte le persone interessate dalla violazione dei dati.

Trasferimento dei dati al di fuori dell'UE

Il regolamento generale sulla protezione dei dati si applica allo Spazio economico europeo (SEE), che comprende tutti i paesi dell'UE più Islanda, Liechtenstein e Norvegia. Quando i dati personali vengono trasferiti al di fuori del SEE, le protezioni offerte dal regolamento devono viaggiare con i dati. Ciò significa che, per esportare dati all'estero, le aziende devono garantire l'esistenza di determinate garanzie.

Il regolamento offre un insieme diversificato di strumenti per il trasferimento dei dati verso paesi terzi. Ai sensi del GDPR, tali trasferimenti sono consentiti quando:

- le protezioni del paese sono ritenute adeguate dall'UE;
- la tua azienda adotta le misure necessarie per fornire garanzie adeguate, ad esempio includendo delle clausole specifiche nel contratto concluso con l'importatore non europeo dei dati personali;
- la tua azienda si avvale di particolari motivi per il trasferimento (denominati «deroghe»), come il consenso della persona.

Devi fare una valutazione d'impatto sulla protezione dei dati?

È obbligatoria la valutazione d'impatto sulla protezione dei dati ogni volta che il trattamento può comportare un rischio elevato per i diritti e le libertà delle persone, ad esempio quando si utilizzano nuove tecnologie.

Lo scopo della valutazione d'impatto sulla protezione dei dati è di identificare i rischi potenziali per i diritti e le libertà delle persone prima dell'inizio del trattamento dei dati e prima che il rischio si concretizzi.

Riducendo il rischio in anticipo, è possibile evitare i danni e ridurre al minimo i costi.

Rispondere alle richieste

Se la tua azienda riceve una richiesta da una persona che vuole esercitare i propri diritti, devi rispondere a tale richiesta senza indebito ritardo e in ogni caso entro un mese dal ricevimento. Questo termine può essere prolungato di due mesi per richieste complesse o multiple, a condizione che l'interessato sia informato della proroga. Inoltre, le richieste devono essere evase gratuitamente. Se respingi la richiesta, devi informare l'interessato dei motivi di tale rifiuto e del suo diritto di presentare un reclamo presso l'autorità per la protezione dei dati.

Dimostra la conformità della tua azienda e conserva i registri!

Uno dei principi fondamentali alla base del regolamento generale sulla protezione dei dati è garantire che le aziende possano dimostrare la loro conformità. Ciò significa che devi essere in grado di dimostrare che la tua azienda agisce in conformità con il regolamento e adempie tutti gli obblighi applicabili, in particolare su richiesta o ispezione da parte dell'autorità per la protezione dei dati.

Un modo per farlo è quello di tenere registrazioni dettagliate su cose come:

- nome e dati di contatto di chi nella tua azienda è coinvolto nel trattamento dei dati
- motivo/i per il trattamento di dati personali
- descrizione delle categorie di persone che forniscono dati personali
- categorie di organizzazioni che ricevono i dati personali
- il trasferimento dei dati personali a un altro paese o organizzazione
- il periodo di conservazione dei dati personali.

Per quanto riguarda il trattamento dei dati personali, il regolamento generale sulla protezione dei dati lascia a te l'iniziativa. Il primo passo è tracciare le attuali attività di trattamento dei dati e riconsiderare i processi aziendali interni In particolare, devi:

- identificare i dati in tuo possesso e stabilire per quali finalità e su quale base giuridica li possiedi
- analizzare tutti i contratti in essere, in particolare quelli tra titolari e responsabili del trattamento
- valutare tutte le vie disponibili per i trasferimenti internazionali
- rivedere la *governance* globale della tua azienda (ovvero quali misure informatiche e organizzative sono in atto), compresa la necessità di nominare o meno un responsabile della protezione dei dati.

Un elemento essenziale di questo processo è garantire che il più alto livello dirigenziale della tua azienda sia coinvolto in tali revisioni, dia il proprio input e venga regolarmente aggiornato e consultato in merito alle modifiche alla politica dei dati.

Per il trattamento transfrontaliero, l'autorità competente può essere un'autorità di vigilanza di un altro paese e non l'autorità per la protezione dei dati del tuo paese. In genere, è l'autorità di protezione dei dati del paese che ospita lo stabilimento principale della tua impresa (dove vengono prese le decisioni sui mezzi e le finalità del trattamento) all'interno dell'UE.

I rischi della non conformità

Il mancato rispetto del regolamento generale sulla protezione dei dati può comportare sanzioni pecuniarie significative: fino a 20 milioni di euro o al 4 % del fatturato globale della tua azienda per determinate violazioni.
L'autorità per la protezione dei dati può imporre ulteriori misure correttive, ad esempio ordinare la cessazione del trattamento dei dati personali. Bisogna poi considerare anche il danno alla reputazione che la mancata osservanza potrebbe causare.
Chiaramente, i costi della mancata conformità al regolamento sono di gran lunga superiori a qualsiasi investimento effettuato per conformarvisi.

Domande? Preoccupazioni?
Consulta l'autorità per la protezione dei dati del tuo paese.
Trova online la tua autorità nazionale per la protezione dei dati
https://ec.europa.eu/newsroom/article29/items/612080

AVVISO IMPORTANTE

Le informazioni e le linee guida contenute in questa brochure hanno lo scopo di contribuire a una migliore comprensione delle norme dell'UE sulla protezione dei dati.
Esse sono intese esclusivamente come strumento di orientamento: solo il testo del regolamento generale sulla protezione dei dati ha forza legale. Pertanto, solo il regolamento può dare luogo a diritti e obblighi per le persone.
Questa guida non dà luogo ad alcun diritto o aspettativa esecutiva.
L'interpretazione vincolante della legislazione dell'UE è di competenza esclusiva della Corte di giustizia dell'Unione europea. Le opinioni espresse in questa guida non possono pregiudicare la posizione che la Commissione potrebbe assumere dinanzi alla Corte di giustizia.
Né la Commissione europea né alcuna persona che agisca per conto della Commissione europea è responsabile per l'uso che può essere fatto delle informazioni contenute nella brochure.
Poiché questa guida riflette lo stato dell'arte al momento della sua stesura, deve essere considerata come uno «strumento vivente» aperto al miglioramento e il suo contenuto potrebbe essere soggetto a modifiche senza preavviso.

FONTE

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2018

A cura di

Exasys Srl
S.P. n. 60 Triggiano - San Giorgio km 0.800
70019, Triggiano (Bari)
080 214 80 12
info@exasys.it
www.exasys.it