GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GUIDA AL NUOVO

REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il Regolamento europeo (UE) 2016/679 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati è entrato in vigore il 24 maggio 2016 e diventerà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018

Più diritti e più opportunità per tutti

Il Regolamento porterà significative innovazioni non solo per i cittadini, ma anche per le aziende, gli enti pubblici, le associazioni, i liberi professionisti

Cittadini più garantiti

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (*data breach)*.

Informazioni più chiare e complete sul trattamento

L’informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all’esercizio dei diritti.

Per facilitare la comprensione dei contenuti, nell’informativa si potrà fare ricorso anche a icone, identiche in tutta l’Unione europea.

Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell’Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Consenso, strumento di garanzia anche on line

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).
Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito».

Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.

Il consenso potrà essere revocato in ogni momento.
I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

I fornitori di servizi Internet e i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Limiti alla possibilità per il titolare di adottare decisioni solo sulla base di un trattamento automatizzato di dati

Le decisioni che producono effetti giuridici (come, la concessione di un prestito) non potranno essere basate esclusivamente sul trattamento automatizzato dei dati (ad esempio, la profilazione).

Faranno eccezione i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati, oppure questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge.

In ogni caso, sono previste garanzie per gli interessati, come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa.

Se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Più tutele e libertà con il diritto all'oblio

Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.

A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.

Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Portabilità dei dati: liberi di trasferire i propri dati in un mercato digitale più aperto alla concorrenza

Il Regolamento introduce il diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro.
Ad esempio, si potrà cambiare il *provider* di posta elettronica senza perdere i contatti e i messaggi salvati.

Ci saranno però alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Garanzie rigorose per il trasferimento dei dati al di fuori dell'Ue

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.

Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.

In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).

Il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi potranno avvenire solo sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Obbligo di comunicare i casi di violazione dei dati personali *(data breach)*

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.);
oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato).
In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un'inserzione su un quotidiano o una comunicazione sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Le novità per le imprese e gli enti

Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni.
In caso di inosservanza delle regole sono previste sanzioni, anche elevate.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Un unico insieme di norme per tutti gli Stati dell’Unione europea

Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell’Unione europea e non richiede una legge di recepimento nazionale.

Inoltre, si applica integralmente alle imprese situate fuori dall’Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell’Unione europea.
Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue.

Fra le principali novità del Regolamento c’è il cosiddetto «sportello unico» (*one stop shop*), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.
Salvo casi specifici, le imprese stabilite in più Stati membri o che offrono prodotti e servizi in vari Paesi dell’Ue, per risolvere possibili problematiche sull’applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all’Autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.

Approccio basato sulla valutazione del rischio che premia i soggetti più responsabili

Il Regolamento promuove la responsabilizzazione (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Il principio-chiave è *«privacy by design»*, ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche. Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (*Data Protection Officer* o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.

In compenso, scompaiono alcuni oneri amministrativi come l'obbligo di notificare particolari trattamenti, oppure di sottoporre a verifica preliminare dell'Autorità i trattamenti considerati «a rischio».

Semplificazioni per i soggetti che offrono maggiori garanzie e promuovono sistemi di autoregolamentazione

Il Regolamento promuove il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione europea (nel caso dell'approvazione da parte della Commissione il codice di condotta avrà applicazione nell'intera Ue).

Il titolare potrà far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi. La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati.

L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

Il Regolamento punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea.

Per saperne di più

www.garanteprivacy.it/pacchettoprotezionedati

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Giugno 2016

La guida ha mere finalità divulgative