GDPR: cosa cambia per gli Ordini Professionali e i Professionisti

ING. ETTORE NARDI
CONSIGLIERE ORDINE INGEGNERI NAPOLI E
RESPONSABILE TRASPARENZA E ANTICORRUZIONE

General data protection regulation

- Il **25 maggio** è entrato ufficialmente in vigore il **GDPR** General data protection regulation, anche detto RGDP (Regolamento generale per la protezione dei dati) in materia di protezione dei dati personali. Regolamento n. 2016/679.
- In quanto Regolamento è applicabile in maniera diretta dai Paesi membri e non ha bisogno di leggi di recepimento, ma solo di un lavoro di armonizzazione con le proprie leggi.

I principi generali del Gdpr

Il regolamento riprende alcuni principi fondamentali già in vigore con la precedente legislazione e ne aggiunge di nuovi.

I principi generali relativi al trattamento dei dati che vengono confermati sono:

- tutela del dati persona e trattamento opportuno
- necessità e proporzionalità: il trattamento deve essere adeguato, pertinente e necessario allo scopo
- durata limitata: il trattamento non può protrarsi a tempo indeterminato
- sicurezza e riservatezza
- rispetto del diritto delle persone

I principi generali del Gdpr

Sono stati, inoltre, introdotti ulteriori principi non presenti nella precedente normativa:

- principio di *accountability* (principio di responsabilizzazione)
- minimizzazione dei dati
- diritto all'oblio
- diritto alla portabilità dei dati
- notificazione tempestiva dei data breach al Garante e agli interessati

A chi si applica il Gdpr

Il nuovo Regolamento si applica a:

- persone
- società
- organizzazioni

che **raccolgono e trattano** (manualmente o mediante procedure automatiche) **qualsiasi tipo di dato personale** in UE.

A chi non si applica il Gdpr

Il regolamento **non si applica** ai trattamenti di dati personali:

- effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione
- effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE
- effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico
- effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica

Cosa si intende per dato personale

Per **dato personale** si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»).

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento al nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità

Cosa si intende per dato personale

Sono **dati personali** tutti gli elementi carattestici dell'identità:

- fisica
- fisiologica
- genetica
- psichica
- economica
- culturale
- sociale

Cosa si intende per dato personale

Il Gdpr aggiunge ulteriori tre tipoligie di dati:

- **Dati genetici**: sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Cosa si intende per dato personale

- **Dati biometric**i: sono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dati relativi alla salute**: sono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Trattamento

Per **trattamento** si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come:

- la raccolta di dati
- la registrazione di dati
- l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione di dati
- l'uso di dati
- la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione,
- la limitazione, la cancellazione o la distruzione di dati

Titolare del trattamento e Responsabile del trattamento

- Il **titolare del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali.**

- Il **responsabile del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento.**

Profilazione

Con il termine profilazione si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti:

il rendimento professionale, la situazione economica, la salute, gli interessi, le preferenze personali, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Consenso

Il consenso dell'interessato è qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso **manifesta il proprio assenso**, mediante **dichiarazione o azione positiva inequivocabile**, che i dati personali che lo riguardano saranno oggetto di trattamento.

Il Gdpr mira ad una **semplificazione** della definizione del consenso: il consenso alla raccolta dei dati e al successivo trattamento da parte degli utenti deve essere fornito in forma chiara, con un atto inequivocabile.

Consenso

Va bene una casella da spuntare.

Non vanno bene:

- caselle precompilate,
- silenzio assenso
- altri meccanismi poco chiari.

L'autorizzazione dovrebbe anche essere **spacchettata**, cioè richiesta per ogni elaborazione che su quelle informazioni sarà effettuata.

Accesso ai dati

I dati in possesso dei titolare devono essere accessibili.

L'utente deve essere messo in condizione di poterne chiedere:

- l'accesso, per conoscere i dati in possesso del titolare
- la rettifica, in caso volesse modificare qualcosa
- la cancellazione, qualora cambiasse idea
- l'approfondimento delle informative sulle finalità e sulle tecniche di profilazione.

Informativa

L'art. 13, del Gdpr impone al titolare di fornire una serie di informazioni, tra cui:

- l'identità e i dati di contatto del titolare e, ove applicabile, del suo rappresentante all'estero
- i dati di contatto del responsabile della protezione dei dati (ove applicabile)
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento
- le categorie di dati personali in questione
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali

Informativa

L'art. 13, del Gdpr impone al titolare di fornire una serie di informazioni, tra cui:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
- i diritti che gli interessati possono esercitare
- le condizioni e le modalità per l'esercizio dei diritti degli interessati
- il diritto di presentare un reclamo all'autorità di controllo
- le informazioni sulla natura normativa o contrattuale del trattamento quando si tratta della base giuridica del trattamento.

Informativa – Chiarimenti del Garante

Alla luce dei chiarimenti resi dal Garante, l'informativa deve:

- avere forma concisa
- essere trasparente, comprensibile per l'interessato
- essere facilmente accessibile

Deve essere scritta in un **linguaggio chiaro** e **semplice** e può essere resa anche in **formato elettronico** (su sito web) o **comunicata via email**.

Conservazione dei dati

Il titolare del trattamento deve definire una **politica** di **durata** e di **conservazione dei dati**.

I dati personali possono essere **conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta**.

Data breach e notifica delle violazioni

Si tratta della **violazione dei dati personali** che comporta, accidentalmente o in modo illecito, la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Ogni violazione dei dati deve essere notificata con informazioni specifiche agli interessati entro **72 ore** (art. 33 del Regolamento).

Viene istituito un registro delle attività nel quale sono registrati nome e dati di contatto del titolare del trattamento, le finalità, le categorie di interessati e di dati raccolti, i trasferimenti di quegli stessi dati verso Paesi terzi o altre organizzazioni, i termini per la cancellazione e una sintesi delle misure di sicurezza adottate.

Il responsabile della protezione dei dati e il controllo

Il **Data Protection Officer (DPO)** o responsabile della protezione dei dati è una figura distinta dal titolare e nasce per garantire la messa in pratica delle diverse norme previste.

La designazione del DPO, ai sensi dell'art. 37 è obbligatoria in tre ipotesi:

- il trattamento di dati personali è effettuato da un'autorità pubblica o da un organismo pubblico
- quando le attività principali dell'organizzazione consistono in trattamenti che, richiedono il "monitoraggio regolare e sistematico" degli interessati "su larga scala"
- quando le attività principali dell'organizzazione consistono nel trattamento "su larga scala" di dati "sensibili" o "giudiziari"

Il responsabile della protezione dei dati e il controllo

Il Responsabile protezione dati (RPD) è un consulente esperto e qualificato che affianca il titolare nella gestione delle questioni connesse al trattamento dei dati personali e lo aiuta a rispettare la normativa vigente.

Tale figura, introdotta per la prima volta nel nostro ordinamento dal Regolamento, ma già diffuso in altri Stati membri, ha un ruolo da tenere ben distinto da quello del responsabile del trattamento, che affianca per compiti e responsabilità il titolare stesso.

Il responsabile della protezione dei dati e il controllo

Il DPO viene designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento.

SOGGETTI ESENTATI DALLA NOMINA DEL RPD

Secondo quanto previsto dal Garante per la protezione dei dati personali, la designazione del responsabile del trattamento non è obbligatoria (è però raccomandata, per dimostrare di essersi responsabilizzati) in relazione a trattamenti effettuati da:

- liberi professionisti operanti in forma individuale
- agenti, rappresentanti e mediatori operanti non su larga scala
- imprese individuali o familiari
- piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti

GDPR: cosa cambia per i Professionisti

- Nel caso di singoli professionisti e piccoli studi le conseguenze del GDPR sono minime e non è prevista la nomina del DPO (Data Protection Officer)
- Gli studi di grandi dimensioni devono dotarsi di un Responsabile della protezione dati, soprattutto se l'attività svolta prevede relazioni internazionali;
- Parimenti deve fare il professionista associato a uno studio o parte integrante di una società tra professionisti.

GDPR: cosa cambia per i Professionisti

Può essere utile, per tutti, redigere un **registro delle attività di trattamento**, dalla semplice raccolta della rubrica clienti alle operazioni di backup del database, che magari implica un passaggio su server esterni

In questo senso è fondamentale valutare la propria politica in tema di **consenso informato e trasparente** al trattamento dei propri dati. Le informative devono essere personalizzate a seconda del tipo di utenti (clienti, fornitori, committenti, etc)

GDPR: Come adeguarsi

1. **ANALISI E RACCOLTA DEI DATI**

Il primo passo consiste in un'**analisi interna** di tutte le aree aziendali, quindi dei dati in possesso, compresi quelli dei dipendenti, partner e fornitori, in modo da poter verificare:

- di quali dati si è in possesso (personali, sensibili, anonimi)
- su quali piattaforme (rete aziendale, web, e-commerce, app,…)
- qual è il livello di sicurezza
- in che modo è stato chiesto il consenso agli utenti iscritti al sito e alla mailing list

GDPR: Come adeguarsi

2. **REDAZIONE DEL REGISTRO DEL TRATTAMENTO DEI DATI:**

Non è obbligatorio per le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato.

Il registro del trattamento dei dati, rappresenta il **punto di partenza fondamentale per il processo di adeguamento** di competenza del titolare del trattamento dei dati e dovrà contenere una serie di dati...

GDPR: Come adeguarsi

…

- nome e dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati
- finalità del trattamento
- descrizione delle categorie di interessati e delle categorie di dati personali
- categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi
- se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione
- termini ultimi previsti per la cancellazione delle diverse categorie di dati
- descrizione generale delle misure di sicurezza tecniche e organizzative

GDPR: Come adeguarsi

3. **ACQUISIRE IL CONSENSO ESPLICITO AL TRATTAMENTO DEI DATI:**

Il consenso alla raccolta dei dati deve essere **concesso liberamente** e deve essere **specifico**, **informato** e **inequivocabile**.

Non può provenire dal silenzio, da caselle preselezionate o dell'inattività.

Occorre prevedere l'informativa (in forma scritta) relativa al diritto di revoca del consenso in qualsiasi momento ed in modo semplice.

GDPR: Come adeguarsi

4. **RISPETTARE IL PRINCIPIO DI ACCOUNTABILITY:**

Si tratta del processo di **responsabilizzazione** verso la tutela e la protezione dei dati personali.

Sulla base di questo principio si distinguono le **due figure di responsabilità** che insieme garantiscono la regolare applicazione del GDPR.

- la redazione e gestione del REGISTRO DEL TRATTAMENTO DEI DATI il quale viene affidato al TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI, ovvero il titolare dell'azienda che risulta tale in virtù del potere di poter disporre dei dati sulla privacy. Questo avrà il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati al fine di garantire una adeguata protezione.

GDPR: Come adeguarsi

5. **VALUTAZIONE DEI RISCHI :**

Ad integrare questo approccio del principio di accountability, basato sulla valutazione del rischio, intervengono i principi di **privacy by design** e **privacy by default**, due concetti innovativi che definiscono:

- Il concetto di **privacy by default** introdotto nel Regolamento evidenzia la necessità della tutela della vita privata dei cittadini "di default", ossia come impostazione predefinita. Questo in occasione di operazioni che portano l'utente a rendere i propri dati a terzi, come nel caso di registrazione a servizi online;
- Il concetto **privacy by design** si basa sul principio prevenire e non correggere; si tratta della necessità di tutelare il dato sin dalla progettazione di sistemi informatici che ne prevedano l'utilizzo.

GDPR: Perché adeguarsi

SANZIONI PREVISTE GDPR

Le SANZIONI AMMINISTRATIVE sono comprese tra i €10.000.000 e i €20.000.000 o dal 2% al 4% del fatturato annuo nel caso in cui siano violati:

- I principi relativi al trattamento e al consenso;
- Disposizioni relative ai diritti dell'interessato;
- Disposizione in materia di trasferimento dati;
- Ordine di cessazione del trattamento.

GDPR: Perché adeguarsi

SANZIONI PREVISTE GDPR

Le SANZIONI PENALI previste variano:

- Da 6 a 18 mesi di carcere per trattamento illecito di dati personali;
- Da 1 a 6 anni di carcere per la diffusione di dati relativi a un numero rilevante di persone;
- Da 1 a 4 anni di carcere per acquisizione di dati relativi a un numero rilevante di persone;
- Da 6 mesi a 3 anni di carcere per falsità nelle dichiarazioni al Garante;
- Arresto da 15 giorni a 1 anno e ammenda fino a 7.700€ per le violazioni in materia di controlli a distanza e indagini su opinioni dei lavoratori.

Guida utile e check list

REDATTA DA : Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino — ORDINE DEGLI AVVOCATI DI TORINO — ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Si articola nei seguenti tre passaggi:

1. Mappatura delle categorie di dati raccolti, trattati e conservati
2. Compilazione (risposte «Sì» o «No»), con possibilità di commenti, ad ogni check di azioni possibili
3. Individuazione, al termine della compilazione, delle misure relative all'adeguato trattamento dei dati non ancora attuate.

Guida utile e check list

Documento

Check list