

General Data Protection Regulation

REGOLAMENTO UE 2016/679

Obblighi in materia di sicurezza e adempimenti della Pubblica Amministrazione (privacy, trasparenza, ecc..)

Prof. Michele Perilli

mlperilli@gmail.com

GDPR (General Data Protection Regulation)

E’ il regime di protezione dei dati personali proposto dalla C.E. per tutti gli stati membri;

- È stato adottato il 27 aprile 2016;
- È andato in vigore dal 25 maggio 2018;
- Non è una direttiva e quindi non c’è stato bisogno di alcuna legislazione applicativa degli stati membri;

GDPR (General Data Protection Regulation)

Sono obbligati ad attenersi al regolamento anche entità che non fanno parte della C.E., ma che hanno dati residenti nei territori degli stati membri della C.E.

Il regolamento non riguarda la gestione di dati personali per attività di sicurezza nazionale o di ordine pubblico.

GDPR (General Data Protection Regulation)

Ogni stato membro istituisce un'autorità per sovrintendere i reclami, le indagini e sanzionare le infrazioni sul trattamento dei dati personali.

Una commissione europea per la protezione dei dati (EDPB, European Data Protection Board) coordina le autorità sovrintendenti degli stati membri.

GDPR (General Data Protection Regulation)

Le Responsabilità:

- Le notifiche sul trattamento dei dati dovranno includere il tempo di mantenimento dei dati;
- Si dovrà comunicare chi controlla i dati e chi protegge i dati;
- Si avrà diritto a contestare le decisioni automatizzate, compresa la profilazione, oggetto di elaborazione algoritmica;
- Non sono inclusi i dati personali necessari ed essenziali per dare vita ad un rapporto contrattuale;

Il Responsabile della Protezione dei Dati Personali

- È un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dei dati;
- Viene designato dal Titolare del Trattamento dei Dati e dal Responsabile del Trattamento dei Dati;
- La designazione è obbligatoria quando:
  - ✓ il Titolare del Trattamento è un'autorità pubblica o un organismo pubblico;
  - ✓ i trattamenti consistono e richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
  - ✓ il trattamento dei dati riguarda su larga scala i dati sensibili e giudiziari.

Accountability

- Incentrato sul titolare del trattamento, colui che ha la responsabilità legale della struttura ed il compito di assicurare il rispetto dei princìpi applicabili al trattamento dei dati personali;
- Non vi è più una serie predefinita di adempimenti da rispettare, ma deve essere ciascun titolare, nell'ambito della propria autonomia e previa accurata valutazione dei rischi, a dover individuare le più idonee e adeguate misure organizzative e tecniche, e a doverne dimostrare l'applicazione e l'efficacia.

Le novità del GDPR rispetto al vecchio codice della privacy D.Lgs. 196/2003

Il raggiungimento dell'obiettivo

- Il titolare dovrà applicare le più adeguate misure tecniche, derivate da un'analisi del contesto della sua attività e da un'analisi dei rischi;
- Non esiste la misura tecnica più adeguata per eccellenza che raggiunge l'obiettivo della sicurezza globale, ma un insieme di misure più idonee ad assicurare i dati in un determinato contesto;
- **Quello che conta è l'obiettivo della sicurezza, non dimostrare di aver applicato un criterio di sicurezza sui dati**

Trasferimento dei dati all'estero

Il regolamento specifica anche il caso del trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale.

Prevede pertanto che l'interessato venga prontamente informato in presenza di una violazione sul trattamento dei dati, che metta a rischio i suoi diritti e le sue libertà.

Diritto all'oblio

Il cosiddetto "*diritto all'oblio*" è il diritto alla cancellazione, limitazione e rettifica dei dati personali e stabilisce che il soggetto ha il diritto di richiedere la cancellazione dei suoi dati personali in caso di mancata osservanza delle norme;

L'interessato deve poter esercitare questo suo diritto con la stessa facilità con cui ha espresso il consenso al trattamento dei suoi dati.

Diritto all'oblio

Il responsabile del trattamento, dietro richiesta dell'interessato, gli dovrà comunicare i destinatari a cui ha trasmesso la sua richiesta di cancellazione.

Sul responsabile del trattamento grava lo stesso onere in caso di richiesta di limitazione o di rettifica dei dati presentata dall'interessato.

Il *"Data Breach"* (violazione di dati personali)

Il titolare del trattamento dei dati avrà l'obbligo legale di comunicare le fughe di dati all'autorità nazionale.

Le denunce di fughe di dati devono essere trasmesse all'autorità sovrintendente non appena se ne viene a conoscenza e comunque entro 72 ore dall'evento.

In alcune situazioni le persone di cui sono stati sottratti i dati dovranno essere avvertite.

Portabilità dei dati

Una persona deve essere in grado di trasferire i propri dati personali da un sistema di elaborazione elettronico a un altro senza che il controllore dei dati possa impedirlo.

I principi generali

Il principio di liceità del trattamento

"i dati personali sono: trattati in modo lecito"

un dato è trattato in modo lecito se rispetta le norme e se è

"l'esecuzione di un compito di interesse pubblico"

Il principio di correttezza

si intende fare riferimento al concetto della buona fede nel trattamento del dato, da parte del Titolare del Trattamento e di tutti gli addetti della struttura che manipola i dati

I principi generali

Il principio della trasparenza

- Il diritto dell'interessato al controllo delle proprie informazioni è ritenuto un punto cardine;
- Bisogna quindi consentire all'interessato il controllo sui dati fornendogli le informazioni relative ai dati trattati, alle finalità del trattamento, all'identità e ai dati di contatto del Titolare, del Responsabile del Trattamento e del Responsabile della Protezione dei Dati;
- Vanno comunicati gli eventuali destinatari dei dati, alla possibilità che i dati vengano trasferiti a un Paese extra UE (cfr. artt. 13 e 14 GDPR);
- Altrettanto importante, in ottica di trasparenza, è informare l'interessato dei diritti che il GDPR riconosce e garantisce, nonché delle modalità attraverso cui esercitarli.

I principi generali

Il principio di pertinenza

- Il principio di pertinenza riguarda il concetto della minimizzazione dei dati richiesti all'interessato.
- I dati devono essere raccolti non in eccedenza rispetto alle finalità Regolamento

Il principio di necessità

Nel principio di necessità si esprime il concetto che i dati sono trattati in quanto necessari. I dati sono quindi necessari ad un ente pubblico/privato per fini istituzionali e per intraprendere un rapporto tra le parti Regolamento UE 2016/679 art. 5, par 1, lett. c)

I principi generali

Il principio di sicurezza

- La sicurezza è un obbligo stringente per coloro che effettuano il trattamento. Già presente nel D.Lgs. 196/2003, il principio si evolve;

- Non è più una sicurezza meramente tecnica, ma è anche l'insieme delle misure organizzative e delle policy per rendere sicuro il trattamento del dato;

- Si parla infatti di sicurezza del sistema *informativo* e non *informatico,* ovvero un insieme non solo di apparecchiature, ma anche di persone, che è necessario sensibilizzare e formare, di procedure aziendali, che devono essere scrupolosamente seguite.

I principi generali

Il principio di necessità

Nel principio di necessità si esprime il concetto che i dati sono trattati in quanto necessari. I dati sono quindi necessari ad un ente pubblico/privato per fini istituzionali e per intraprendere un rapporto tra le parti Regolamento UE 2016/679 art. 5, par 1, lett. c)

L’interessato

L’interessato al trattamento è la persona fisica alla quale si riferiscono i dati personali e al quale il GDPR riconosce una serie di diritti (indicati negli artt. dal 15 al 22) finalizzati a garantire una trasparenza nei rapporti con il titolare e la possibilità di esercitare un controllo effettivo su tutte le informazioni che lo riguardano, nonché delle modalità attraverso le quali le stesse sono trattate

I diritti dell'interessato

Diritto all'accesso

- L'art. 15 del GDPR riconosce all'interessato il diritto di *"ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali"*

Diritto all'aggiornamento dei dati

- Il diritto all'aggiornamento dei dati, previsto dall'art. 16 del GDPR, consiste nella possibilità, per l'interessato di ottenere che i suoi dati, oggetto di trattamento, siano costantemente aggiornati da parte del titolare. Questo diritto viene esercitato attraverso una richiesta di rettifica dei dati inesatti o non più attuali e l'integrazione di quelli incompleti.

I diritti dell'interessato

Diritto alla cancellazione (diritto all'oblio)

L'interessato ha il diritto di chiedere la cancellazione dei dati che lo riguardano.

Quando si può chiedere la cancellazione ?

- Quando i dati non siano più necessari alla finalità per la quale sono stati raccolti o trattati;
- Quando l'interessato abbia revocato il consenso (nel caso in cui esso sia il solo fondamento di liceità del trattamento);
- Quando i dati siano stati trattati illecitamente o debbano essere cancellati per adempiere a un obbligo legale cui è soggetto il titolare del trattamento;
- Quando i dati siano stati raccolti nell'ambito di servizi offerti dalla società dell'informazione.

I diritti dell'interessato

Diritto di limitazione del trattamento

Con l'art. 18 il GDPR riconosce all'interessato il diritto di ottenere la limitazione del trattamento dei dati che lo riguardano, al verificarsi di determinate condizioni:

- l'interessato contesta l'esattezza dei dati
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- i dati sono necessari all'interessato per esercitare o difendere un diritto in giudizio benché non più necessari al titolare del trattamento in relazione alla finalità perseguita;
- L'interessato si è opposto al trattamento in attesa della verifica circa l'eventuale prevalenza dei motivi legittimi del titolare rispetto ai suoi.

I diritti dell'interessato

Diritto alla portabilità dei dati

L'art. 20 del GDPR introduce un'assoluta novità:

- il diritto alla portabilità dei dati, in base al quale l'interessato ha il diritto di ricevere i dati personali che lo riguardano, in un formato strutturato, di uso comune e leggibile da dispositivo automatico.
- L'interessato ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti dal primo titolare, qualora ricorrano cumulativamente due condizioni: il trattamento si basi sul consenso (anche in relazione alle particolari categorie di dati di cui all'art. 9) o sia necessario per eseguire un contratto e avvenga con mezzi automatizzati.
- Questo diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e non può dunque essere esercitato nei confronti delle pubbliche amministrazioni.

I diritti dell'interessato

Diritti di opposizione

- L'art. 21 del GDPR riconosce all'interessato il diritto di opporsi al trattamento dei propri dati personali in qualsiasi momento e per motivi anche non connessi all'eventuale illegittimità del trattamento. Quando l'interessato esercita tale diritto il titolare deve interrompere il trattamento, a meno che non riesca a dimostrare l'esistenza di motivi legittimi in grado di prevalere sugli interessi e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
- **Specifica disciplina è invece prevista per l'ipotesi in cui i dati personali siano trattati per finalità di marketing diretto. In tale ipotesi l'interessato può esercitare il diritto di opposizione in qualsiasi momento e senza essere vincolato al bilanciamento con gli interessi di cui è portatore il titolare, poiché evidentemente, nella concezione del legislatore europeo, la finalità commerciale è sempre subordinata alla volontà dell'interessato di opporsi, che pertanto prevale in ogni caso. In tale caso pertanto il titolare deve obbligatoriamente interrompere il trattamento.**

Il trattamento automatizzato e la profilazione

L'art. 22 del GDPR parla del *"processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione",* sancisce il diritto per l'interessato di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, se tale decisione è in grado di incidere sulla sua persona. La norma in esame non vieta l'adozione di processi automatizzati, né della profilazione (intesa come processo in grado di valutare aspetti personali relativi a una persona fisica al fine di prevederne aspetti riguardanti ad esempio le preferenze o gli interessi personali, il comportamento, la situazione economica etc...), ma consente all'interessato di sottrarsi a una decisione che sia basata unicamente su tale modalità di trattamento e che si riverberi sulla sua persona o sia in grado di produrre effetti giuridici che lo riguardano.

Il trattamento automatizzato e la profilazione

Tale diritto non è esercitabile nelle ipotesi in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto in cui una delle parti sia l'interessato, quando sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare o si basi sul consenso esplicito dell'interessato.

Si pensi ai casi di graduatorie elaborate anche attraverso sistemi informatici, quali ad esempio quelle della mobilità del personale docente immesso in ruolo o assunto a tempo indeterminato dal MIUR.

Le figure di responsabilità

Il Titolare del Trattamento (Data controller)

- Il titolare del trattamento dei dati, è la persona fisica, giuridica, autorità pubblica, servizio o altro organismo che singolarmente o insieme ad altri soggetti governa finalità e mezzi dell'intero trattamento e che disciplina le attività di raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione e, infine, cancellazione o distruzione dei dati personali;
- Il titolare del trattamento (data controller) non viene designato da nessuno

Le figure di responsabilità

Responsabile del trattamento (Data processor)

- Il responsabile del trattamento dei dati personali, che non deve essere confuso con la figura del Responsabile della protezione dei dati o Data Protection Officer, è un soggetto che riveste una posizione predominante nell'impianto del GDPR per la sua funzione. Egli è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- Il responsabile del trattamento, a differenza del titolare, non partecipa alla definizione delle finalità e dei mezzi del trattamento, ma deve attenersi alle istruzioni del titolare per il trattamento di cui sia stato incaricato da parte di quest'ultimo.

Le figure di responsabilità

Responsabile del trattamento (Data processor)

- Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate alla protezione del dato personale trattato per conto del titolare.
- Le istruzioni al responsabile del trattamento sono conferite dal titolare mediante atto contrattuale in cui sono individuati:
  - Gli obblighi per il responsabile del trattamento;
  - La durata del trattamento;
  - La natura e la finalità del trattamento;
  - Il tipo di dati personali e le categorie di interessati;
  - Gli obblighi e i diritti del titolare del trattamento.

Le figure di responsabilità

L'incaricato del trattamento

- Il GDPR non prevede espressamente la figura dell'incaricato del trattamento. L'art. 29 prevede anche che i soggetti (incaricati), che si trovino sotto l'autorità del titolare o del responsabile di trattamento, possano trattare i dati personali solo se istruiti in tal senso. Si tratta di una categoria di soggetti che possono continuare a essere definiti, per semplicità, incaricati (o, meglio, autorizzati) al trattamento dei dati personali da parte del titolare o del responsabile. Nell'ottica del rispetto del principio di *accountability* e, soprattutto, della necessità di dimostrare, a posteriori, la conformità al GDPR del trattamento di dati personali effettuato dal titolare o dal responsabile, sarà consigliabile tenere "traccia" sia dell'autorizzazione al trattamento sia delle istruzioni fornite a tali autorizzati.

Tipi di dati e trattamento previsti dal GDPR

- **Definizione di trattamento** : "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, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto".*
- **Dato Personale** : *"qualsiasi informazione riguardante una persona fisica identificata o identificabile" (interessato).*
- **Categorie particolari di dati personali** : si intendono i dati atti a rivelare *"l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"*.
- **Dati personali relativi a condanne penali e reati:** *"dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza".*

La pseudonimizzazione

La pseudonimizzazione

- La ***pseudonomizzazione*** è "il *trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive";*
- La ***pseudonimizzazione*** è un trattamento volto a separare i dati dalla persona alla quale si riferiscono. I dati personali vengono trattati, ma non si è in grado di ricondurli direttamente all'interessato.

Il GDPR, relativamente alle informazioni aggiuntive recita testualmente: *"a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".*

L'informativa

Per esigenza di trasparenza, l'informativa da fornire all'interessato, si amplia rispetto al D.Lgs. 196/2003, introducendo nuove informazioni, in particolare:

- I dati di contatto del Responsabile della Protezione dei Dati Personali;
- La base giuridica del trattamento;
- L'indicazione se sia previsto il trasferimento di dati in Paesi extra-UE (e nel caso attraverso quali strumenti);
- Il periodo di conservazione dei dati (o quantomeno i criteri previsti per stabilire la durata della conservazione);
- Il diritto di presentare reclamo all'Autorità di controllo (Garante);
- Se il trattamento comporti processi decisionali automatizzati (e nel caso la logica dei processi decisionali e le possibili conseguenze per l'interessato).

Il Responsabile della Protezione dei Dati Personali

I compiti di questa nuova figura, indicati nell'art. 39 del GDPR, sono i seguenti:

- Informare e fornire consulenza al titolare o al responsabile nonché ai dipendenti in merito agli obblighi derivanti dal GDPR e dalle altre disposizioni rilevanti, anche con riguardo alla tenuta del Registro dei trattamenti;
- Sorvegliare sull'osservanza del GDPR e delle altre disposizioni rilevanti, e delle politiche adottate dal titolare o dal responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e agli audit;

Il Responsabile della Protezione dei Dati Personali

- Fornire, se richiesto, un parere in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;

- Cooperare con il Garante e fungere da punto di contatto per il Garante per questioni connesse al trattamento ed effettuare.

Il registro delle attività di trattamento

Contiene

- Il nome e i dati di contatto del Titolare del Trattamento (o del responsabile) e quelli del Responsabile della Protezione dei Dati Personali;
- La finalità del trattamento (non prevista per il responsabile per ovvie ragioni);
- Una descrizione delle categorie di interessati e dei dati personali trattati;
- I trasferimenti di dati verso Paesi terzi;
- I termini ultimi previsti per la cancellazione dei dati (ove possibile);
- Una descrizione generale delle misure di sicurezza adottate a tutela dei dati.

Sono esonerati dall'obbligo di tenuta di tali registri le imprese e le associazioni con meno di 250 dipendenti, a meno che il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato, nel caso inoltre in cui il trattamento non sia occasionale o riguardi le categorie particolari di dati o dati relativi a condanne penali o reati.

La valutazione d'impatto sulla protezione dei dati

La valutazione d'impatto sulla protezione dei dati è un processo che ha la funzione di descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti da esso, valutando detti rischi e determinando le misure per affrontarli. **E' un adempimento che non va posto in essere** sempre e comunque, ma deve essere preventivamente effettuato in specifiche ipotesi, previste dal GDPR e in particolare **quando** un tipo di trattamento, allorché **prevede in particolare l'uso di nuove tecnologie**, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.