GDPR - General Data Protection Regulation

Indice

Introduzione

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli ordinamenti degli Stati membri il Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.

Il regolamento GDPR si pone l'obiettivo di eliminare la frammentazione delle normative nazionali e garantire uniformità di disciplina a livello europeo. Esso risponde alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali dei cittadini UE.

Contesto normativo precedente al GDPR

Di seguito è rappresentato il contesto normativo nazionale esistente prima dell'emanazione del Regolamento (UE) 2016/679:

Direttiva n. 95/46/CE

Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

DPR 28 luglio 1999 n. 318

Tutela delle persone fisiche e di altri soggetti rispetto al trattamento dei dati personali.

Legge 31 dicembre 1996 n. 675

Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali.

Direttiva n. 2002/58/CE (e-Privacy)

Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.

DEFINIZIONI PRINCIPALI

Il GDPR si applica ai dati personali.

DATI PERSONALI	Qualsiasi informazione concernente una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line, o a uno o più elementi caratteristici della sua identità fisica, genetica, psichica, economica, culturale, sociale, giudiziaria.
DATI PERSONALI PARTICOLARI	Dati personali che rivelino l'origine razziale, etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, dati relativi alla salute, vita sessuale o orientamento sessuale della persona.
DATI PERSONALI GENETICI	Dati 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.
DATI BIOMETRICI	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	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.

RUOLI E RESPONSABILITA' DI GDPR

Ruoli e Responsabilità definiti nel Regolamento GDPR sono seguenti:

TITOLARE DEL TRATTAMENTO

La persona fisica o giuridica, l'Autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali;

DATA PROTECTION OFFICER

Tutti i soggetti pubblici, devono nominare il Responsabile della protezione dei dati personali. E' la nuova figura di riferimento per le imprese e la Pubblica Amministrazione, per utenti e clienti, ed è l'interfaccia per le Autorità garanti (esclusi i tribunali)

RESPONSABILE DEL TRATTAMENTO

La persona fisica o giuridica, l'Autorità pubblica, il servizio o qualsiasi altro organismo che tratta i dati personali per conto del titolare

DELEGATO E SUBDELEGATI

Il delegato al Trattamento è la persona fisica che rappresenta il Titolare per quanto riguarda gli obblighi relativi alle norme del GDPR.
I Responsabili pro-tempore delle funzioni organizzative di primo livello sono identificati come Delegati al Trattamento.

RUOLI E RESPONSABILITA'

Le caratteristiche delle figure principali nell'ambito GDPR:

TITOLARE DEL TRATTAMENTO

- ✓ Può nominare il DPO
- ✓ Determina le finalità e i mezzi del trattamento di dati personali
- ✓ Comunica eventuali violazioni dei dati personali (data breach) all'Autorità nazionale di protezione dei dati
- ✓ In caso di violazione dei dati personali valuta l'effettivo rischio per gli interessati e ha l'obbligo di informarli qualora vi sia un "rischio elevato" per i loro diritti e libertà.

DATA PROTECTION OFFICER

- ✓ Riferisce al vertice gerarchico del Titolare o del Responsabile del trattamento
- ✓ Rispetta il requisito dell'indipendenza e dell'assenza di conflitto di interessi
- ✓ Ha un ruolo di indirizzo e controllo.

RESPONSABILE DEL TRATTAMENTO

- ✓ Ha una sua responsabilità diretta nella conduzione dei trattamenti e sono previsti più controlli da parte del Titolare
- ✓ E' responsabile dell'attuazione delle misure di sicurezza
- ✓ Non ricorre ad altro Responsabile senza autorizzazione del Titolare
- ✓ È responsabile della compliance normativa per il trasferimento dati

AUTORITA' GARANTE

AUTORITA' GARANTE	Autorità amministrativa indipendente, istituita per il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali

Il Garante si occupa di:

- verificare la conformità alla legge dei trattamenti e prescrivere ai titolari le misure da adottare;
- esaminare i reclami;
- limitare, sospendere o vietare i trattamenti in violazione delle norme;
- adottare le autorizzazioni generali;
- promuovere codici di deontologia e buona condotta (es. in materia di giornalismo);
- partecipare alle attività comunitarie e internazionali (anche quale componente dell'EDPB);
- irrogare sanzioni correttive.

European Data Protection Board

EUROPEAN DATA PROTECTION BOARD

è l'organismo che ha sostituito il Gruppo di lavoro articolo 29 (Working Party article 29 o WP29, appunto perché previsto dall'art. 29 della direttiva europea 95/46), col nuovo regolamento europeo, ed è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati.

È un organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una volta. Il Gruppo adotta le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo.

Il suo compito principale è garantire il principio di congruità e coerenza, cioè assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia. Nell'ambito dell'attuazione del principio del one stop shop, se la decisione di un'autorità di controllo capofila viene contestata da altra autorità di controllo, è l'EDPB a fungere da tribunale di ultima istanza.

European Data Protection Board

Compiti principali di European Data Protection Board

- assicura l'applicazione corretta del regolamento fatti salvi i compiti delle autorità nazionali di controllo;
- fornisce consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione;
- pubblica linee guida, raccomandazioni e prassi al fine di promuovere l'applicazione coerente del regolamento e sulle materie previste;
- esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del regolamento;
- effettua l'accreditamento di organismi di certificazione e il suo riesame periodico;
- fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale;
- promuove la cooperazione e l'effettivo scambio di informazioni e prassi tra le autorità di controllo a livello bilaterale e multilaterale;
- promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;
- emette pareri sui codici di condotta;
- tiene un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

PRINCIPI DI GDPR

ACCOUNTABILITY

Il titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi e deve dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy.

PROPORZIONALITÀ

I dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

CONSENSO

Il consenso deve essere, in tutti i casi, libero, specifico, informato e inequivocabile. La forma scritta è la modalità più idonea a configurare l'inequivocabilità del consenso.

PRIVACY BY DESIGN

Il Titolare o Responsab. del trattamento deve prevedere la messa in atto di adeguate misure e procedure tecniche con l'obiettivo di contemplare gli aspetti privacy in ogni attività legata ai dati personali. In aggiunta devono garantire che siano trattati di default solo i dati necessari per ciascuna finalità specifica del trattamento, e che la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite.

RISK-BASED APPROACH

Valutazione dei rischi derivanti dai trattamenti ritenuti critici.
Le imprese, inoltre, possono effettuare un Data Protection Impact Assessment.
In tal modo, l'implementazione delle misure di sicurezza adottate terrà conto dell'analisi dei rischi e dei costi di attuazione.

DIRITTI DEGLI AUTORI PRINCIPALI DI GDPR

DIRITTO DI RETTIFICA

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

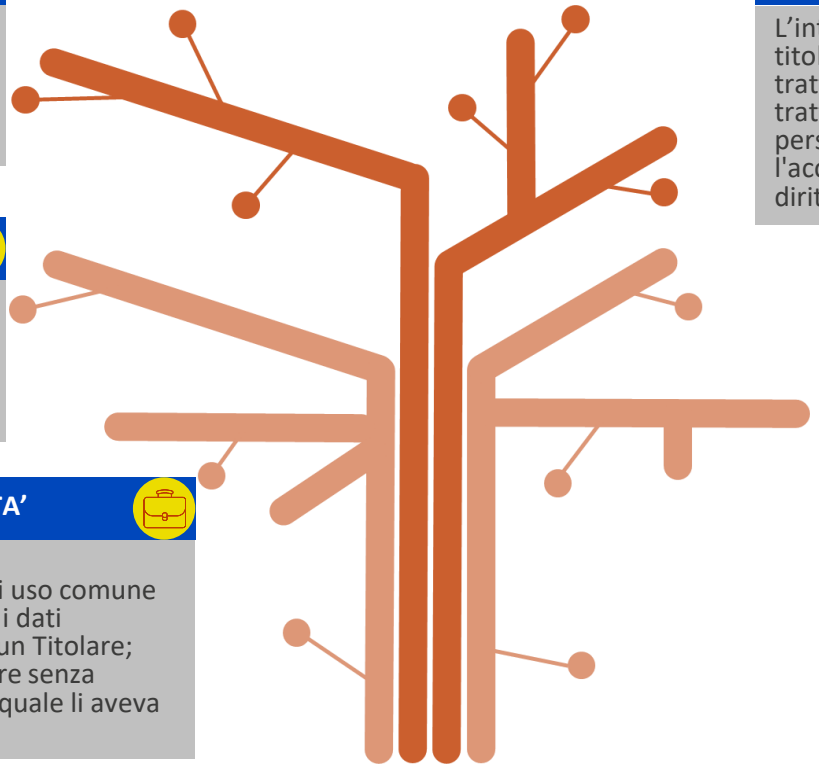
DIRITTO ALL'OBLIO

Il Titolare del trattamento deve: garantire all'interessato la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (Right to be forgotten).

DIRITTO ALLA PORTABILITA'

L'interessato ha il diritto di:

- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare;
- trasmettere tali dati a un altro Titolare senza impedimenti da parte del Titolare al quale li aveva forniti.



DIRITTO DI LIMITAZIONE AL TRATTAMENTO

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento (ad esempio, nei casi di trattamento illecito o quando i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria).

DIRITTO DI OPPOSIZIONE

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.

Casi: GDPR, data breach e security

- Autorità nazionale di vigilanza della Romania ha multato per 130.000 euro Unicredit Bank per violazione dell'art. 25, art. 5 e del considerando 78. Unicredit non avrebbe applicato in modo efficace **le misure tecniche e organizzative necessarie per garantire un'ottimale protezione dei dati**.

- La Cnil, l'autorità nazionale francese per la protezione dei dati, ha sanzionato Google per 50 milioni di euro con l'accusa di aver violato alcuni obblighi nel quadro del regolamento UE per la protezione dei dati personali (artt. 13-14).

GDPR e autorità giudiziaria: **D.lgs. 51/2018** (attuazione della direttiva 680/2016 su trattamenti di pubblica sicurezza)

Sono esclusi dall'ambito di applicazione del **D.lgs. 51/2018** (attuazione della direttiva 680/2016 su trattamenti di pubblica sicurezza) i trattamenti di **dati personali effettuati nell'ambito di attività concernenti la sicurezza nazionale e tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea** e, in particolare, attività afferenti la politica estera e la sicurezza comune, così come sancito dal titolo V, capo 2, del TUE.

Il decreto legislativo 51/2018 si applica anche ai trattamenti di dati personali effettuati dall'autorità giudiziaria (Procure della Repubblica comprese) ma il legislatore italiano, facendo valere la clausola di flessibilità ha scelto di non sottoporre i trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle sue funzioni giurisdizionali al controllo del Garante per la protezione dei dati personali al fine di salvaguardarne l'indipendenza.

GDPR e autorità giudiziaria: principi

Principi di trattamento applicabili

I dati personali reperiti nel contesto penale e di sicurezza - viene sancito nel D.lgs. 51/2018 - vanno:

- trattati in modo lecito e corretto;
- raccolti per **finalità determinate**, espresse e legittime e trattati in modo compatibile con tali finalità;
- adeguati, pertinenti e **non eccedenti rispetto alle finalità** per le quali sono trattati;
- esatti e, se necessario, **aggiornati**;
- conservati con modalità che consentano l'**identificazione** degli **interessati per il tempo necessario** al conseguimento delle finalità per le quali sono trattati, sottoposti a **esame periodico per verificarne la persistente necessità** di conservazione, cancellati o anonimizzati una volta decorso tale termine;
- trattati in modo da garantire un'**adeguata sicurezza e protezione** da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, mediante l'adozione di misure tecniche e organizzative adeguate.

GDPR e autorità giudiziaria: applicabilità

Art. 4 (in attuazione degli artt. 6 e 7 direttiva 680/2016 su trattamenti di pubblica sicurezza): il titolare del trattamento, tenuto conto delle finalità e per quanto possibile, deve tenere distinti i dati personali a seconda che siano fondati su fatti o su valutazioni nonché di differenziarli in relazione ai soggetti interessati, categorizzati, sulla scorta della terminologia tecnica adottata dal codice di procedura penale, in: persone sottoposte ad indagine, imputati (anche in relazione a procedimenti connessi o collegati), condannati in via definitiva, persone offese, parti civili, persone informate sui fatti e testimoni.

Art. 8: divieto assoluto di *automated decision-making*, salvo si tratti di un processo decisionale automatizzato espressamente autorizzato dal diritto dell'Unione o dello Stato membro, i quali prevedano adeguate garanzie per i diritti e libertà dell'interessato. Una tutela ancor più rigorosa viene accordata alle decisioni automatizzate che si basano su categorie particolari di dati (dati personali già definiti sensibili nel codice privacy, oltre a quelli genetici e biometrici), le quali debbono essere subordinate ad adeguate misure di salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato.

GDPR e autorità giudiziaria: applicabilità

Art. 26: tutti i *data breach* (**salvo per i trattamenti effettuati dall'autorità giudiziaria nell'esercizio delle sue funzioni giurisdizionali**) debbono essere notificati al Garante senza alcuna eccezione e, se si tratta di dati trasmessi o ricevuti da un altro Stato membro, la notifica deve essere fatta anche al relativo titolare in tale Stato membro. Nel caso in cui la violazione comporti un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione dovrà essere inviata anche agli interessati, salvo sia necessario un suo differimento nel tempo per ragioni di tutela della sicurezza pubblica o nazionale, dei diritti e delle libertà altrui ed al fine di non compromettere il buon esito di un'attività di prevenzione, indagine o accertamento in corso.

Capo IV (artt.31-36): I presupposti che delimitano il perimetro di liceità dei trasferimenti all'estero sono particolarmente stringenti e sono rappresentati da cinque condizioni: 1) necessità del trasferimento per raggiungere le finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali; 2) trasferimento ad un'autorità competente straniera che persegua le stesse finalità; 3) autorizzazione al trasferimento dello Stato membro di provenienza per dati da questo provenienti e successivamente trasmessi all'estero; 4) sussistenza di una decisione di adeguatezza della Commissione europea; 5) necessità di una valutazione di adeguatezza nell'ipotesi di trasferimento successivo ad un altro Paese terzo od ad altra organizzazione internazionale.

GDPR e autorità giudiziaria

TRATTAMENTO DATI SENSIBILI, GENETICI, BIOMETRICI, RELATIVI ALLA SALUTE.

Sebbene il loro trattamento sia generalmente vietato, il GDPR esplicita una **deroga** qualora esso sia necessario per **accertare, esercitare e difendere un diritto in sede giudiziaria e ogni qualvolta le autorità giurisdizionali esercitino la loro funzioni.**

Le Pubbliche amministrazioni hanno l'obbligo di nominare il DPO e di adeguarsi alle altre prescrizioni di regolamento. Ad esempio, gli avvocati in quanto difensori potranno esercitare anche una "vigilanza" sul rispetto delle garanzie e tutele.

A completamento dei principi previsti dal GDPR, secondo il D.lgs. 51/2018 (attuazione della direttiva 680/2016 su trattamenti di pubblica sicurezza):

- I dati personali in ambito penale sono conservati per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti ad esame periodico per verificarne la persistente necessità di conservazione e cancellati o anonimizzati una volta decorso il termine previsto.
- Inoltre, in ambito giudiziario, la tutela degli interessati è quindi assicurata, per le parti, dalle garanzie che riconoscono i diritti di difesa all'interno del procedimento penale, anche con riguardo ai dati personali necessariamente oggetto di trattamento, assicurando quindi la possibilità di limitare l'esercizio dei diritti dell'interessato, conformemente alle esigenze di prevenzione, di indagine e processuali.
- Per garantire i diritti in ambito giudiziario anche con riferimento ai terzi, si è previsto uno speciale procedimento attraverso il quale qualsiasi interessato, durante il procedimento penale o dopo la sua definizione, può chiedere la rettifica, la cancellazione o la limitazione dei dati personali che lo riguardano.

Approfondimento

Libri di testo, risorse web e altri materiali di approfondimento

- Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
- Garante per la protezione dei dati personali, “REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI. Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018”, 2018