G.D.P.R. a scuola.

La normativa e le buone pratiche per la sicurezza dei dati

Cosa è il GDPR

General Data Protection Regulation

Regolamento generale sulla protezione dei dati

Regolamento (UE) 2016/679

Attuazione: 25 Maggio 2018

Introduzione al GDPR

«[...] Non domandarci la formula che mondi possa aprirti, sì qualche storta sillaba e secca come un ramo.
Codesto solo oggi possiamo dirti,
ciò che *non* siamo, ciò che *non* vogliamo.»

Eugenio Montale

Importanza dei dati

Le origini del GDPR

- Direttiva 95/46/CE (24/10/1995)
- L. 675/1996 (31/12/1996)
- D.lgs. 196/2003
- Regolamento (UE) 2016/679
- D.lgs. 101/2018 (10/08/2018)

Le origini del GDPR

Carta dei diritti fondamentali dell'Unione europea

Articolo 8

Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Le origini del GDPR

Trattato sul funzionamento dell'Unione europea

Articolo 16

(ex articolo 286 del TCE)

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.

Le origini del GDPR

Trattato sull'Unione europea (TUE)

Articolo 39

Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

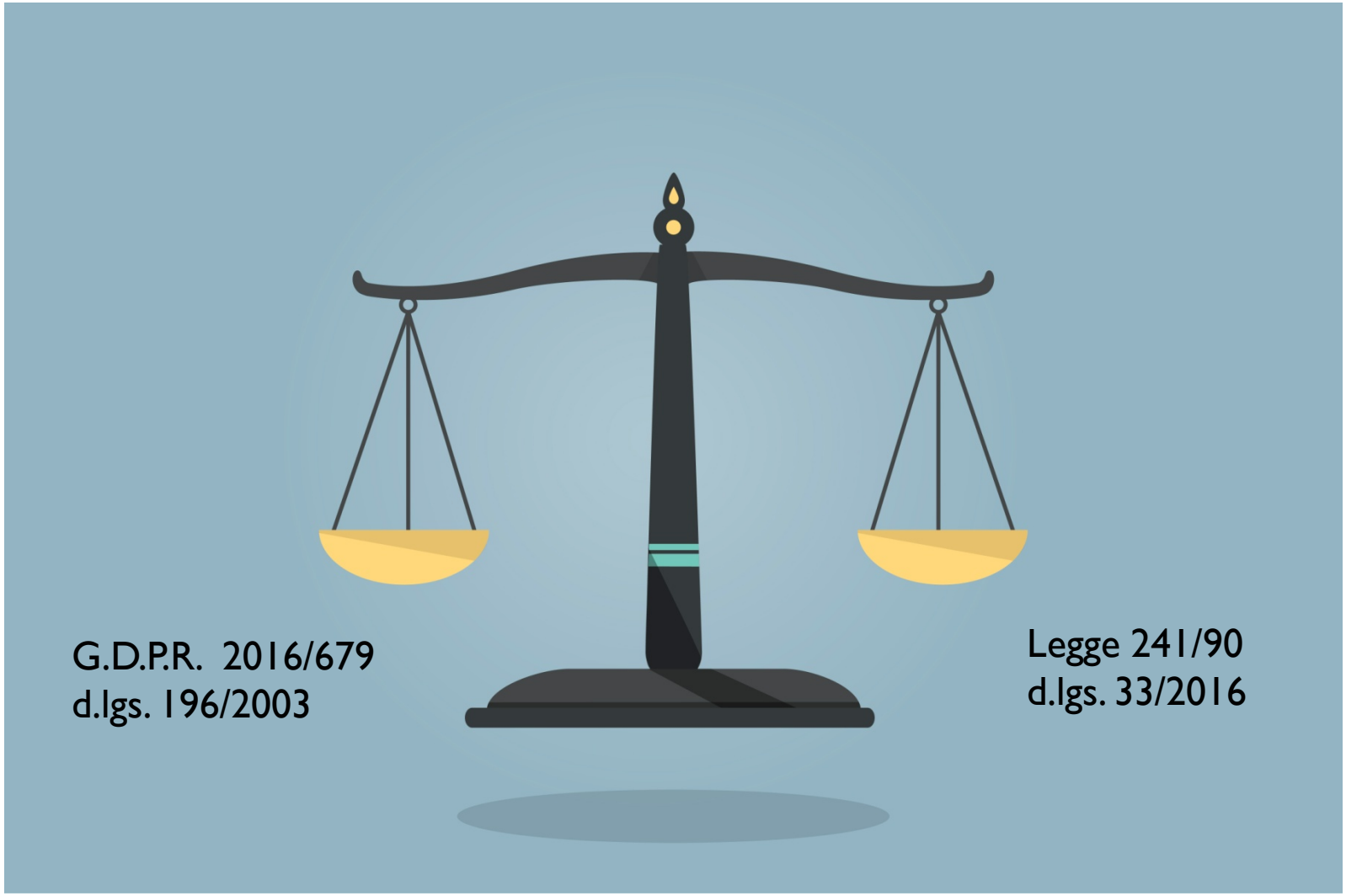
Normativa di riferimento

GDPR
regolamento UE
2016/679

Adeguamento GDPR
Dlgs 101/2018

Codice della Privacy
Dlgs 196/2003

Privacy e Trasparenza



Novità del GDPR

- Niente misure «minime»
- Diritto all'oblio (gli utenti possono chiedere di rimuovere informazioni a proprio riguardo)
- «portabilità» dei dati
- Obbligo di notifica in caso di data breach (gli enti, se subiscono violazione dei dati, devono comunicarlo entro 72 ore).
- Figura del D.P.O.

Cosa si rischia?

Sanzioni pecuniarie

Sanzioni Amministrative Pecuniarie (83 GDPR)

- Sanzioni di minore entità, che possono raggiungere i 10 milioni di euro per i singoli e per le aziende fino al 2% del fatturato globale annuo riguardanti la violazione degli obblighi previsti per i titolari ed i responsabili.
- Sanzioni di maggiore entità, che possono arrivare a 20 milioni di euro per i singoli o fino al 4% del fatturato mondiale annuo per le aziende, a prescindere da dove sia la sede principale che può essere anche fuori dall'Europa.

Sanzioni penali

Sanzioni penali

Vengono introdotti reati più specifici in relazione al "Trattamento dei dati". Le sanzioni prevedono misure che vanno da 6 mesi fino ad arrivare ai casi più gravi a 6 anni di reclusione

"…Chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dal Regolamento arreca nocumento all'interessato, sarà punito" per i reati di:

- **Trattamento illecito di dati** (reclusione da 1 a 3 anni);
- **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala** (reclusione da 1 a 6 anni);
- **Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala** (reclusione da 1 a 4 anni);
- **Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante** (da 6 mesi a 3 anni);
- **Inosservanza dei provvedimenti del Garante** (da 3 mesi a 2 anni).

GDPR

I termini più usati

Dato personale

«dato personale»: 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 a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Trattamento

«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 o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Interessato

E’ il «proprietario» del dato personale.

Una persona fisica, identificata o identificabile a cui fanno capo i dati oggetto del trattamento.

Titolare del trattamento

«titolare del trattamento»: 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; […]

Risponde al Garante e all'interessato del trattamento dei dati personali.

Responsabile del trattamento

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Esempi:
Mensa, Amministratore di rete, Software house gestionali, Assistenza informatica, Fornitore Cloud, RSPP, Altri…

Autorizzati al trattamento

Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art. 30 del Dlgs. n. 196/2003), il regolamento UE non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"

"*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali* ***non può trattare tali dati se non è istruito in tal senso dal titolare*** …" art.29 G.D.P.R.

La formazione può essere realizzata mediante: Lettere, mansionario, disciplinare interno, corsi, regolamento interno.

D.P.O. o R.P.D.

Il responsabile della protezione dei dati (data protection officer) è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) Cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36,ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Principi del trattamento

Principio di liceità

Art. 6 del GDPR, il trattamento è lecito se:

- **consenso esplicito** dell'interessato al trattamento per finalità determinate dei propri dati;
- l'adempimento di obblighi assunti con un **contratto** di cui l'interessato è parte o l'esecuzione di attività precontrattuali dallo stesso richieste;
- l'adempimento di obblighi imposti dalla **legge** in capo al titolare;
- la tutela di **interessi essenziali** per la vita dell'interessato o di soggetti terzi (si pensi, ad esempio, a casi di trattamento a fini umanitari o in caso di epidemie);
- rilevanti motivi di **interesse pubblico** correlati all'esercizio di pubblici poteri;
- il perseguimento di un **interesse legittimo** del titolare o di un'altra persona fisica ritenuto **prevalente** sui diritti e sulle libertà fondamentali dell'interessato, realizzabile attraverso il trattamento di dati personali.

Correttezza

Sintetizzabile nel concetto di Buona fede in tutte le fasi del trattamento dei dati.

Principio di trasparenza

La trasparenza è una qualità richiesta alle modalità con cui vengono raccolti e utilizzati i dati personali. Il Regolamento richiede che tali informazioni siano facilmente accessibili e che le comunicazioni relative al trattamento siano comprensibili.

- Quali dati sto trattando?
- Quali sono le finalità?
- Quali sono le modalità?
- Chi è il titolare? E chi il DPO ?
- A chi verranno trasmessi i dati? Anche fuori EU?
- Quali sono i diritti dell'interessato rispetto ai dati trattati?

Limitazione della finalità

La raccolta dei dati degli utenti dovrà avvenire soltanto per finalità determinate, esplicite e legittime, e che il trattamento conseguente a tale raccolta dovrà essere effettuato con modalità compatibili con tali finalità.

Minimizzazione dei dati

Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Principio della esattezza

I dati raccolti devono essere esatti e, se necessario, aggiornati. Di conseguenza gli enti dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

Limitazione della conservazione

I dati possono essere conservati esclusivamente per il tempo necessario al raggiungimento delle finalità per le quali sono trattati.

Possono essere trattati più a lungo solo ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. (In questo caso devono essere messi in atto in maniera particolare)

Integrità e riservatezza

I dati devono essere trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

Accountability

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. (Art. 24 GDPR)

Accountability:

- Responsabilizzazione
- Abilità di dare conto
- approccio proattivo per fare in modo che le cose funzionino

Gli strumenti operativi

Il registro dei trattamenti

Titolare ed eventuale Responsabile, possono compilare il **Registro delle attività di trattamento** svolte dall'organizzazione.

Il Registro del titolare deve contenere

- nome e contatti del Titolare, del suo Rappresentante e, se del caso, del Responsabile della protezione dei dati;
- le finalità del trattamento, inclusi gli eventuali legittimi interessi;
- la descrizione delle categorie di interessati;
- la descrizione delle categorie di dati;
- le categorie di eventuali destinatari, inclusi quelli collocati in paesi terzi
- (non UE);
- la documentazione delle garanzie adeguate per tutti i trasferimenti verso i paesi terzi
- I termini di cancellazione dei dati personali;
- la descrizione generale delle misure di sicurezza tecnico-organizzative.

L'informativa

E' il documento fondamentale per instaurare il rapporto tra titolare e interessato, deve essere personalizzato rispetto alla propria organizzazione e deve essere sottoposto all'interessato ogni volta che si raccolgono, direttamente o indirettamente, dati personali.

Deve indicare:

- **l'identità e i dati di contatto del titolare del trattamento e, se presente, del responsabile della protezione dei dati personali**
- **le finalità**
- **la durata**
- **le basi di legittimità del trattamento (principio di liceità)**
- **gli eventuali destinatari dei dati personali**
- in caso di trasferimenti verso paesi terzi o organizzazioni internazionali, dettagli in merito al luogo di trasferimento e all'esistenza di garanzie adeguate per la tutela dei loro diritti
- **le possibili conseguenze di un mancato conferimento dei dati personali**
- l'eventuale utilizzo di strumenti di profilazione o l'esistenza di decisioni automatizzate che lo riguardano
- **la possibilità di esercitare i diritti previsti e la possibilità di proporre reclami**

Consenso

Raccolta e gestione del consenso

Necessario per effettuare trattamenti di dati personali;

Non va richiesto in presenza di una idonea base normativa.

In generale è sempre richiesto nel caso di trattamento di dati personali:

- rientranti tra le categorie particolari di dati personali (origine razziale o etnica, relativi alla salute, alla religione, all'appartenenza sindacale, ecc.)
- relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Comunque, per trattare questi dati, sono richieste speciali cautele e il trattamento può essere effettuato solo se i dati indicati sono indispensabili per l'attività istituzionale svolta.

Nomine

Tutti coloro che:

- trattano dati personali
- ricevono dati personali
- entrano in contatto con dati personali nell'erogazione di un contratto di servizio

Devono:

- Ricevere opportuna formazione
- Eventualmente operare in virtù di un contratto o di un atto giuridico vincolante che stabilisca chiaramente compiti, responsabilità e confini del trattamento
- essere selezionati in base alle proprie competenze, sulla base del principio di responsabilizzazione del titolare

Privacy by design & by default

Privacy by design: I problemi vanno valutati nella fase di progettazione, e la raccolta dei dati deve prevenire il verificarsi dei rischi;

Privacy by default: Gli enti dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti

Casi di studio

Casi di studio:

- Ragazzi in gita
- Foto presso manifestazioni
- Problematica foto degli alunni quando vanno via dalla scuola
- Richiesta questura
- Dati eccedenti (titoli di studio o professione dei genitori)
- Docente ripreso davanti ad altre persone
- Note disciplinari devono essere riservate
- Stampa unione
- File zip con password