Introduction to Data Protection

Diamo una rapida occhiata a com'era la scena legale in Europa prima dell'arrivo del GDPR. In particolar modo, prima del GDPR, vi era la **direttiva** del **1995**, che essendo una direttiva non è immediatamente applicabile in tutti gli stati europei → questo comporta, che ciascun stato europeo doveva definirsi autonomamente una legge, che definiva come le organizzazioni (in quello stato) dovessero trattare i dati personali dei cittadini ed ovviamente, questo ha comportato il fatto, che ogni stato trattava i dati personali dei cittadini in maniera diversa. Il GDPR (nel 2018) ha sostituito la direttiva del 1995 ed in particolare, il GDPR è un **regolamento** e come tale, può essere immediatamente applicato → quindi, non vi è la necessità, che uno stato definisca una propria legge sul trattamento dei dati.

Un altro importante cambiamento, è che quando era in vigore la direttiva del 1995, l'ente che si occupava (a livello europeo) di supervisionare l'applicazione degli stati della direttiva, era il **Working Party 29** → con l'entrata in vigore del GDPR, tale ente è stato sostituito dall'**European Data Protection Board (EDPB)**, il quale è formato da tutte le entità (responsabili a livello nazionale di ciascun stato europeo) per la protezione dei dati personali (come per esempio, in Italia il garante della privacy).

> 💡 L'obiettivo del GDPR, quindi è u**niformare i principi, secondo cui un'organizzazione appartenente alla comunità europea, deve trattare i dati personali dei cittadini**.

Sorge la domanda: "**A chi si applica il GDPR?**" Viene applicato a tutte le organizzazioni, che processa dati personali di **individui** residenti nella comunità europea → da notare, che è stato utilizzato il termine individuo e non cittadino, in quanto con il termine "individui", comprendiamo anche le organizzazioni (in questo modo, anche un'organizzazione americana che opera in suolo europeo, la quale tratta i dati dei cittadini, è soggetta al GDPR).

Sorge a questo punto spontanea la domanda: "**Cosa sono i dati personali?**" Il GDPR, specifica che i dati personali, sono tutte quelle informazioni relative ad un individuo, che lo identificano in maniera diretta oppure indiretta. Per esempio, le informazioni che identificano in **maniera diretta** un individuo sono:

- nome;
- cognome;

- indirizzo;
- codice fiscale;
- numero patente.

Le informazioni, invece, che identificano in **maniera indiretta** un individuo possono essere:

- indirizzo IP.

esse, quindi, descrivono il comportamento dell'individuo, in maniera tale che l'individuo può essere distinto dagli altri individui ed inoltre combinando tali informazioni con altre informazioni in possesso delle organizzazioni (che raccolgono informazioni sugli individui) si è in grado di risalire all'identità dell'individuo.

"**Chi è coinvolto nel processamento dei dati personali?**" Principalmente sono coinvolte tre entità:

1. il **soggetto interessato** → ovverosia il cittadino, i cui dati personali vengono raccolti ed analizzati da determinate organizzazioni;
2. il **titolare del trattamento** (detto anche **data controller**) → ovverosia l'organizzazione e/o l'entità giuridica, che decide per quali motivi, per quali finalità e con quali mezzi, vengono raccolti i dati del soggetto interessato. In alcuni casi, il titolare del trattamento può delegare il trattamento e/o l'analisi e/o la memorizzazione dei dati ad un'altra organizzazione, ovverosia il **responsabile del trattamento**;
3. il **responsabile del trattamento** → prima dell'entrata in vigore del GDPR, vi era una sostanziale differenza negli obblighi e nelle responsabilità che avevano il titolare del trattamento e il responsabile del trattamento, per quanto riguarda il trattamento dei dati personali. Con l'entrara in vigore del GDPR, entrambi hanno le stesse responsabilità per quanto riguarda il trattamento dei dati personali.

Vediamo un esempio per capire chi ricopre queste tre entità: "Un'agenzia di viaggi invia i dati personali dei propri clienti alle compagnie aeree e a una catena di alberghi, al fine di effettuare le prenotazioni per un pacchetto di viaggio. La compagnia aerea e l'hotel confermano la disponibilità dei posti e delle camere richieste. L'agenzia di viaggi emette i documenti di viaggio e i voucher per i suoi clienti". Chi è il data controller? In questo caso, il data controller è:

- l'agenzia di viaggi;
- la compagnia aerea;

- la catena di hotel.

Tutti e tre, quindi, rappresentano il data controller.

“**Cosa deve fare un titolare del trattamento per processare i dati personali dei propri utenti?**” Vi sono una serie di obblighi (per precisione 8), che il data controller deve rispettare. In particolare questi obblighi sono:

1. per trattare i dati (quindi per raccogliere, analizzarli e memorizzare i dati), il titolare del trattamento deve avere una **base giuridica**, ovverosia una motivazione legale valida per processare i dati. Il GDPR prevede sei basi giuridiche valide, che sono:
    a. il **consenso** → l'interessato (= l’utente) ha dato il consenso al trattamento dei suoi dati personali per una o più finalità specifiche. Per consenso dell'interessato si intende qualsiasi **manifestazione di volontà libera, specifica, informata e inequivocabile** (= **non ambigua**) con la quale l'interessato, mediante una dichiarazione o una chiara azione affermativa, manifesta il proprio assenso al trattamento dei dati personali che lo riguardano. In particolare, con:
        i. **volontà libera** → intendiamo che la fornitura del servizio, non deve essere condizionata dal fatto che l’utente presti il proprio consenso a trattare i propri dati personali;
        ii. **volontà specifica** → l’utente deve poter dare il proprio consenso, per trattare i propri dati personali, per ogni finalità e attività di trattamento (quindi l’utente può concedere il trattamento dei propri dati personali per alcune finalità e per altre no);
        iii. **volontà informata** → spiegare in un linguaggio chiaro e conciso:
            1. il nome del responsabile del trattamento dei dati;
            2. il nome di eventuali terzi responsabili del trattamento che si baseranno sul consenso;
            3. finalità del trattamento;
            4. eventuali attività di trattamento;
            5. informare le persone che possono ritirare il consenso in qualsiasi momento.
        iv. **volontà inequivocabile** → il silenzio oppure le caselle pre-selezionate o l'inattività non devono costituire un consenso. Il consenso, quindi, è

valido se solamente se corrisponde ad un’azione positiva fatta dal soggetto interessato.

b. il **contratto** → il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte e per stipulare tale contratto, l’interessato deve fornire (al data controller) i propri dati personali (quali ad esempio: nome, cognome, indirizzo);

c. l’**obbligo legale** → il trattamento è necessario per l'adempimento di un obbligo legale a cui il titolare del trattamento è soggetto (per esempio, il titolare del trattamento ha venduto un oggetto ad un individuo e per legge, il titolare deve fare una fattura. Per fare la fattura, il titolare deve raccogliere i dati dell’individuo);

d. **interesse vitale** → il trattamento è necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica;

e. **pubblico interesse** → il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento;

f. **interesse legittimo** → il trattamento è necessario ai fini dei legittimi interessi perseguiti dal responsabile del trattamento o da un terzo, salvo che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

2. i dati devono essere seguire il **principio di limitazione della finalità**, ovvero i dati devono essere trattati per uno scopo specifico e limitato, nel senso che: se il titolare del trattamento raccoglie i dati per un certo scopo, non può utilizzarli successivamente per un altro scopo diverso da quello iniziale (per esempio, il dottore raccoglie i dati del paziente per fornirli una determinata cura. Successivamente, il dottore non può condividere tali dati del paziente con un amico, in modo tale che quest’ultimo fornisca al paziente, ad esempio, dei pacchetti viaggio);
3. i dati devono seguire il **principio di data-minimization**, ovvero un titolare del trattamento dovrebbe sempre e solo raccogliere i dati, che sono strettamente necessari per il conseguimento di un determinato obiettivo (per esempio, un’organizzazione cerca del personale per ricoprire una determinata posizione all’interno dell’organizzazione. Durante il colloquio, l’organizzazione dovrebbe chiedere all’individuo, solamente le informazioni inerenti al posto di lavoro (come ad esempio: il titolo di studio o le competenze linguistiche) e non altre

informazioni sensibili non pertinenti (come ad esempio: l'orientamento politico o sessuale));

4. i dati devono seguire il **principio di limitazione della conservazione**, ovvero che il titolare del trattamento deve mantenere una copia dei dati, dei soggetti interessati, solo per il tempo necessario per raggiungere la finalità per cui erano stati raccolti (riprendendo l'esempio di prima, una volta assunto il nuovo dipendente, l'organizzazione deve cancellare i dati dei vari candidati);
5. i dati devono seguire il **principio di accuratezza dei dati**, ovvero che il titolare del trattamento è obbligato a mantenere una copia, sempre aggiornata e corretta, dei dati personali dei soggetti interessati;
6. i dati devono seguire il **principio di sicurezza dei dati**, ovvero che il titolare del trattamento ha l'obbligo di adottare tutte le misure di protezione, che garantiscono che i dati personali dei propri clienti, dipendenti e fornitori, siano protetti da attacchi che vanno a violare la confidenzialità, la riservatezza, la disponibilità e l'integrità dei dati. Oltre a ciò, il GDPR impone al titolare, di notificare (in un tempo molto breve) ai clienti, dipendenti e fornitori di essere stati soggetti di un attacco informatico;
7. il titolare del trattamento deve **facilitare** l'esercizio dei diritti dei soggetti interessati, rispetto al trattamento dei dati personali;
8. i dati devono seguire il **principio di responsabilizzazione**, ovvero che il titolare del trattamento deve dimostrare (mediante una serie di attività) che esso (ovvero il titolare) processa i dati secondo i principi visti fino a questo momento (per fare ciò, ad esempio è obbligo per l'organizzazione mantenere un registro dei trattamenti).

Un ulteriore aspetto introdotto dal GDPR è di dare maggiore conoscenza e controllo ai soggetti interessati, in riguardo a quali sono le azioni che può effettuare sul trattamento dei propri dati personali. In particolare, abbiamo:

1. il primo diritto è quello di essere informato → esso va a pari passo con il requisito che riguarda il consenso. Secondo questo primo diritto, il titolare del trattamento deve presentare al soggetto interessato (prima di raccogliere i dati e quindi prima di iniziare qualsiasi trattamento dei dati) un'informativa della privacy e/o una privacy policy. Inoltre, il regolamento prevede:
    a. quali informazioni devono essere contenute nell'informativa della privacy e/o nella privacy policy (come per esempio: il nome del titolare del trattamento,

la finalità, la base giuridica, le tipologie di dati raccolte dal sito e se i dati vengono condivisi);

   b. con quale modalità devono essere fornite le informazioni. Il GDPR suggerisce alcuni modi, con cui la politica diventa più leggibile e usufruibile per il soggetto interessato (per esempio: utilizzare icone grafiche e adottare politiche che sono strutturate a più livelli di dettaglio delle informazioni e quindi al 1° livello si hanno le informazioni necessario, al 2° livello le informazioni più dettagliate e così via).

2. il secondo diritto è quello di richiedere l'accesso ai propri dati. Secondo questo diritto, quindi, un utente può chiedere all'organizzazione se quest'ultima ha una copia dei propri dati personali e in caso, può richiedere una copia di tutti i propri dati personali mantenuti dall'organizzazione. Inoltre, l'organizzazione deve fornire all'utente tutte le informazioni su come i dati vengono trattati;
3. il terzo diritto è quello della portabilità dei dati → in base a questo diritto, se un utente vuole cambiare il fornitore di un servizio, può richiedere a quest'ultimo di fornirgli una copia dei propri dati personali, oppure di trasferirli direttamente all'altro fornitore di servizi;
4. il quarto diritto riguarda la cancellazione dei dati → in questo caso, il soggetto interessato può richiedere al titolare del trattamento, di cancellare la copia dei propri dati personali. Questo, però, **non è un diritto assoluto**, ovvero questo diritto vale solamente quando la base giuridica (per trattare i dati) è il **consenso** e quindi, tale diritto si applica se::

   a. il soggetto interessato, quindi, ha revocato il consenso del trattamento dei propri dati personali;

   b. il titolare del trattamento, non tratta i dati del soggetto interessato, secondo i principi previsti dal GDPR.

5. infine, abbiamo i diritti legati alla possibilità del soggetto interessato di interrompere oppure di opporsi ad un trattamento effettuato dal titolare del trattamento. Anche in questo caso, vi sono delle specifiche condizioni, per cui il soggetto interessato può interrompere o opporsi al trattamento, come per esempio:

   a. se il titolare del trattamento utilizza algoritmi di machine learning per prendere decisioni per l'utente, quest'ultimo può opporsi al trattamento e di conseguenza, il titolare del trattamento deve interrompere il trattamento.

Sorge, infine, una domanda: “**Cosa succede se avviene un Data breach?**” Un’organizzazione deve essere in grado di fornire (nel giro di 72 ore) tutte le informazioni relative all’attacco di cui è caduta vittima. In Italia, tali informazioni devono essere fornite al Garante della Privacy. In particolare, nella valutazione dell’attacco, l’organizzazione deve specificare:

- l’impatto negativo dell’attacco;
- quali misure sono state adottate dall’organizzazione per contenere gli effetti dell’attacco;
- se l’attacco ha comportato una violazione dei diritti di privacy degli utenti.

Nel caso in cui l’organizzazione **non** fornisca tali informazioni al Garante della Privacy, il GDPR prevede due livelli di sanzioni:

1. pagare una **sanzione** di, al massimo, **10 milioni** di euro, oppure il **2%** del fatturato annuale dell’organizzazione;
2. pagare una **sanzione**, di al massimo, **20 milioni** di euro, oppure al **4%** del fatturato annuale dell’organizzazione.