Seminario 1

Protezione dei dati nel mondo universitario

Definizione. Un **dato personale** è una qualsiasi informazione riguardante una persona fisica **identificata** o **identificabile** direttamente o indirettamente.

Questi dati, essendo collegabili all'identità di una persona, richiedono particolari attenzioni e protezioni per garantire la privacy e la sicurezza dell'individuo, in linea con quanto espresso dal GDPR (C26, C27, C30).

Consideriamo **dati personali** (ex Dati sensibili) tutti quei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute, alla vita sessuale o al suo orientamento sessuale.

Il GDPR

Il **Regolamento Generale sulla Protezione dei Dati** (RGPD o GDPR, dall'inglese *General Data Protection Regulation*), ufficialmente noto come **Regolamento (UE) n. 2016/679**, è una normativa dell'Unione Europea dedicata alla tutela della privacy e al trattamento dei dati personali. Entrato in vigore nel 2016 per rafforzare la protezione dei dati dei cittadini europei, il GDPR stabilisce le regole su come le aziende e le organizzazioni devono raccogliere, gestire, archiviare e proteggere le informazioni personali, garantendo trasparenza, sicurezza e rispetto dei diritti individuali in un contesto sempre più digitalizzato e interconnesso.

Il GDPR ha come obiettivo principale:

- **Proteggere i diritti e le libertà fondamentali delle persone fisiche**, con particolare attenzione al diritto alla protezione dei dati personali, assicurando che ogni individuo possa mantenere il controllo e la riservatezza sulle proprie informazioni.
- **Favorire la libera circolazione dei dati personali all'interno dell'Unione Europea**, consentendo alle informazioni di spostarsi liberamente tra Stati membri in modo sicuro e regolamentato, senza compromettere la privacy dei cittadini e sostenendo la crescita economica del mercato digitale europeo.

Ambito di applicazione

Il GDPR si applica a diverse tipologie di trattamento dei dati personali, con un ambito di applicazione ben definito che include:

- **Trattamento automatizzato o parzialmente automatizzato dei dati personali**, ovvero ogni processo svolto con l'ausilio di strumenti informatici o digitali.
- **Trattamento non automatizzato dei dati personali contenuti in un archivio** o destinati ad essere archiviati, che include anche i dati conservati in formato cartaceo o in archivi manuali organizzati.
- **Titolari del trattamento situati nell'Unione Europea**, indipendentemente dal luogo in cui avviene il trattamento effettivo dei dati.
- **Titolari del trattamento situati al di fuori dell'UE** ma che trattano i dati di persone fisiche presenti nell'UE, ad esempio nel caso di servizi digitali o vendite internazionali.
- **Esclusione dei trattamenti effettuati per uso strettamente personale**, dove i dati non sono destinati a una comunicazione sistematica né all'accesso di terze parti.

Cosa cambia davvero?

1. **Dal consenso al controllo**: Gli individui acquisiscono maggiore controllo sui propri dati personali, con diritti più chiari e strumenti per esercitarli (es. accesso, rettifica, cancellazione).
2. **Accountability del Titolare**: Il Titolare è responsabile di definire finalità e mezzi del trattamento, garantire la conformità al GDPR e dimostrarla attraverso misure adeguate, assicurando trasparenza e legalità.
3. **Figura del DPO**: Il GDPR istituisce la figura del **Responsabile della Protezione dei Dati (DPO)**, una figura chiave per garantire il rispetto delle normative sulla protezione dei dati personali.

Principi del GDPR

I **principi del GDPR** costituiscono le basi per il trattamento dei dati personali in modo conforme e responsabile. Essi sono:

1. **Liceità, correttezza e trasparenza**: I dati devono essere trattati legalmente, in modo chiaro e comprensibile per gli interessati.
2. **Limitazione delle finalità**: I dati possono essere raccolti solo per scopi specifici, espliciti e legittimi, e non utilizzati per fini incompatibili con tali scopi.
3. **Minimizzazione dei dati**: Devono essere trattati solo i dati strettamente necessari rispetto alle finalità per cui sono raccolti.
4. **Correttezza**: I dati devono essere accurati e, se necessario, aggiornati; quelli errati devono essere rettificati o cancellati.
5. **Limitazione della conservazione**: I dati devono essere conservati solo per il tempo necessario al raggiungimento delle finalità per cui sono stati raccolti.

6. **Misure di Sicurezza**: Devono essere adottate misure di sicurezza adeguate per proteggere i dati da accessi non autorizzati, perdite o danni.
7. **Responsabilizzazione (Accountability)**: Il titolare del trattamento deve dimostrare la conformità al GDPR attraverso misure tecniche e organizzative adeguate.

Misure di sicurezza

Il GDPR mette a disposizioni misure di sicurezza per il trattamento dei dati personali:

- **Psudonimizzazione**: Cioè il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Le informazioni aggiuntive necessarie dovranno essere conservate separatamente e soggette a misure tecniche e organizzative per garantire che non siano attribuiti a una persona fisica identificata o identificabile. L'identificabilità di un soggetto andrà valutata in base al costo e ai tempi richiesti per l'identificazione, comprendendo anche le tecnologie disponibili e i possibili sviluppi tecnologici.
- **Dati anonimi**: Sono informazioni che non si riferiscono a una persona fisica identificata o identificabile o sono dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Quindi **l'identificabilità non deve essere possibile con alcun mezzo**.

Quindi possiamo dire che i dati **pseudoanonimi** sono ancora considerati dati personali, mentre i dati anonimi no. Essendo questi ultimi non considerati dati personali, non sono soggetti ai regolamenti del GDPR per il trattamento dei dati personali.

Trattamento dei dati nella ricerca scientifica

Il GDPR riconosce il ruolo fondamentale della ricerca scientifica per il progresso dell'umanità, ma non autorizza il trattamento indiscriminato dei dati. Ogni trattamento dei dati deve essere pensato per:

- Trattare solo i dati necessari allo scopo (minimizzazione)
- Proteggere i dati durante il trattamento (Sicurezza)
- Distruggere i dati nel momento in cui non sono più necessari per le finalità della ricerca scientifica
- Prediligere dati anonimi per sottrarli dall'applicazione del GDPR

Quindi possiamo dire che le regole essenziali sono tre:

1. Se il dato personali non serve, cancellalo o distruggilo
2. Se serve il dato ma non il riferimento alla persona, **anonimizzalo**

3. Se i primi due punti non sono praticabili, dimostra quello che puoi e non puoi fare per raggiungere gli obiettivi della ricerca.

In questi caso come altri in cui vi è un trattamento bisogna mettere in pratica il **DPIA** (Data Protection Impact Assessment, o Valutazione d'Impatto sulla Protezione dei Dati), uno strumento previsto dal **GDPR** per valutare e mitigare i rischi legati al trattamento dei dati personali, soprattutto quando questo trattamento può comportare un rischio elevato per i diritti e le libertà delle persone. Le fasi sono articolate nel seguente modo:

1. **Descrizione del trattamento**: Obiettivi della ricerca, dati trattati, modalità di raccolta e utilizzo.
2. **Valutazione dei rischi**: Analisi delle possibili minacce per la sicurezza e la privacy.
3. **Mitigazione dei rischi**: Identificazione delle soluzioni per proteggere i dati (ad esempio, anonimizzazione).
4. **Documentazione**: Produzione di un rapporto che dimostri la conformità al GDPR.