UNIVERSITÀ DEL SALENTO

FAQ – PRIVACY

FAQ 1. Qual è l'ambito di applicazione del nuovo Regolamento europeo (GDPR 679/2016)?

Il Regolamento europeo si applica in relazione al trattamento dati di persone fisiche, e non giuridiche, in modalità automatizzata e non, ed è vincolante nei Paesi membri dell'UE. Le disposizioni si applicano a tutti gli Stati dell'UE e risultano vincolanti anche per le imprese situate fuori dall'Unione europea che offrono servizi o prodotti all'interno del mercato UE.

2. Che cosa significa Accountability?

Con l'entrata in vigore del nuovo regolamento europeo in materia di protezione dei dati personali GDPR 679/2016 ha, infatti, determinato un radicale cambiamento nell'approccio adottato nella regolamentazione della materia, introducendo nel sistema legislativo di settore principi prima estranei al nostro ordinamento ed attribuendo, tra questi, un ruolo di preminente centralità e di guida a quello così detto di "*responsabilizzazione*" del titolare e del responsabile del trattamento. Il termine in lingua inglese utilizzato dal Legislatore europeo per esprimere il concetto di cui si parla è quello di "*accountability",* che trova in italiano la traduzione più adatta in*"responsabilizzazione",* l'interessato deve ricevere cioè

tutte le informazioni necessarie per comprendere il trattamento e le sue finalità.

3. Come si manifesta e raccoglie il consenso per il trattamento?

Il consenso è il risultato di un comportamento attivo o di una dichiarazione positiva dell'interessato. Ci sono differenti modalità di raccolta del consenso: dichiarazione scritta, mezzi elettronici, dichiarazione orale. È escluso il silenzio-assenso, così come le caselle preselezionate su internet e, nel complesso, le forme inattive.

3.1 Quando si può parlare di consenso esplicito?

Si parla di consenso esplicito nel momento in cui il consenso è manifestato chiaramente per tutti i casi previsti nel trattamento, con un atto positivo inequivocabile e consapevole da parte dell'interessato. Il consenso esplicito è richiesto principalmente in relazione al trattamento dei dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione)

4. Cos'è la profilazione del dato?

La profilazione consiste nell'attività di raccolta e di elaborazione "automatizzata" dei dati, con lo scopo di valutare determinati aspetti personali relativi a una persona fisica. Il concetto viene esteso rispetto al precedente Codice in materia di privacy, considerando l'Interessato (persona fisica) e quanto a lui direttamente riferibile (età, sesso, situazione economica, stato familiare, etc.), ma anche quanto lo circonda o con cui interagisce. **5. Cos'è la valutazione di impatto sulla protezione dati (DPIA)?**

È una procedura che mira a descrivere un trattamento dati, con l'obiettivo fondamentale di valutarne l'effettiva necessità, la proporzionalità ed i rischi.

5.1 Chi è responsabile della DPIA?

La responsabilità della DPIA spetta al titolare del trattamento, che procede con questa procedura prima di iniziare il trattamento e consultandosi con il responsabile della protezione dati, se designato.

5.2 Quando la DPIA è obbligatoria e quando non lo è?

Il Gruppo di lavoro Art. 29 ha identificato specifichi casi di obbligatorietà e di non obbligatorietà. Quelli in cui la DPIA è obbligatoria comprendono: - trattamenti valutativi o di scoring, compresa la profilazione; decisioni automatizzate con effetti giuridici; - monitoraggio sistematico (es. videosorveglianza); - trattamento di dati sensibili, giudiziari o estremamente personali; - trattamento di dati personali su larga scala; - Big Data; - dati di soggetti vulnerabili; - utilizzo di tecnologie innovative (es. riconoscimento facciale); - trattamenti che potrebbero impedire agli interessati di esercitare un diritto o un servizio o un contratto.

Quelli in cui la DPIA è invece non obbligatoria comprendono trattamenti che: - non presentano rischio elevato; - sono simili altri per cui è già stata condotta una DPIA; - già verificati dall'Autorità di controllo; - sono compresi nell'elenco facoltativo;

- riferiti a norme per cui è già stata condotta una DPIA in fase di definizione. In ogni caso la DPIA può essere richiesta quando si prevede un rischio elevato per i diritti e le libertà delle persone fisiche. Qualora necessaria, la valutazione d'impatto va avviata già nella fase di progettazione del trattamento.

6. Cosa si intende per minimizzazione del dato?

È un principio fondamentale di protezione, il quale prevede che i dati raccolti siano adeguati, pertinenti e limitati a quanto esattamente necessario rispetto alle finalità del trattamento previsto, senza eccedenze.

7. Cosa si intende per pseudonimizzazione del dato?

È una modalità di trattamento dei dati personali che non permette di attribuirli ad un interessato specifico, senza l'utilizzo di informazioni aggiuntive. È da intendersi come una misura di riduzione dei rischi per gli interessati e un aiuto per i titolari e i responsabili del trattamento a rispettare i loro obblighi di protezione dati.

8. Cosa sono i "Dati particolari" menzionati dal nuovo Regolamento?

Il Regolamento definisce "dati particolari" i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita sessuale e l'orientamento sessuale della persona.

Sono compresi anche i "dati sensibili" così come intesi dal precedente Codice.

9. Quali nuove categorie di dati particolari sono introdotti dal Regolamento europeo?

Il Regolamento introduce le nuove categorie "Dati genetici" e "Dati biometrici", definendo poi espressamente i "Dati sanitari". Per dati genetici si intendono quelli relativi alle caratteristiche genetiche, in grado di fornire informazioni su fisiologia o salute dell'interessato e che risultano dall'analisi di un campione biologico. Per dati biometrici si intendono quelli relativi alle caratteristiche fisiche, fisiologiche o comportamentali di un interessato, tali da consentire o confermare la sua precisa identificazione, come l'immagine facciale o i dati dattiloscopici.

10. Chi è la figura del titolare del trattamento dati?

È la persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o altro organismo che, raccoglie i dati personali per proprie finalità e determina le modalità del trattamento.

11. Chi è la figura del responsabile del trattamento dati?

Persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati personali per conto e secondo gli indirizzi forniti dal titolare del trattamento, in base ad un contratto o altro atto giuridico apposito.

11.1 Quali adempimenti gli spettano?

Adotta le più adeguate misure di sicurezza, garantisce il rispetto delle regole e della riservatezza e assiste il titolare durante il trattamento.

11.2 Qualora sia presente un altro responsabile del trattamento, chi ha la responsabilità finale?

Il responsabile del trattamento può ricorrere ad un altro responsabile per l'esecuzione di specifiche attività precisate mediante apposito contratto o altro atto giuridico e assicurando conformità al Regolamento. La responsabilità in solido circa l'adempimento degli obblighi da parte dell'altro responsabile spetta, in ogni caso, al responsabile iniziale.

12. L'Università può essere responsabile del trattamento?

Sì, l'Università può essere responsabile del trattamento mediante le figure che, al suo interno, ricoprono funzioni di particolare rilievo organizzativo o cariche istituzionali. Nel dettaglio, risultano responsabili del trattamento i Dirigenti delle Aree e i Responsabili gestionali dei Dipartimenti, Capiservizio ed autorizzati per lo svolgimento di questa funzione dal Direttore Generale.

13. Cosa si intende per contitolare del trattamento dati?

Persona fisica o giuridica che decide e determina in condivisione con il titolare le finalità ed i mezzi del trattamento. Tramite un accordo interno, sono stabilite le rispettive responsabilità in

merito agli obblighi da osservare, all'esercizio dei diritti dell'interessato e all'informativa.

14. Cos'è il Data breach e quali conseguenze può comportare?

È una violazione di sicurezza che ha come principale conseguenza accidentale o in modo illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato ai dati trasmessi. Ciò comporta effetti negativi significativi sugli individui, che possono tradursi in danni psicologici, materiali e immateriali.

14.1 Quali sono le tipologie di Data breach?

Le violazioni dei dati possono essere classificate in base a tre principi di sicurezza: - "violazione di riservatezza" dove c'è un accesso non autorizzato; - "violazione di integrità" dove c'è una modifica non autorizzata o accidentale; - "violazione di disponibilità" dove c'è una perdita o una distruzione accidentale o non autorizzata.

15. Quali sanzioni sono previste dal nuovo Regolamento europeo?

In caso di mancato rispetto delle norme del Regolamento, sono previste sanzioni effettive, proporzionate e dissuasive. Nel dettaglio, sono previste sanzioni amministrative pecuniarie fino a 10.000 euro per la violazione di obblighi specifici previsti e fino a 20.000 euro per il mancato rispetto degli obblighi fissati dall'Autorità di controllo/Garante.