Gruppo di lavoro CODAU

Linee Guida Privacy e GDPR - Trattamento dei dati personali in ambito universitario

Regolamento UE 2016/679:

principali novità ed azioni di adeguamento richieste

CODAU
Convegno dei Direttori generali
delle Amministrazioni Universitarie

Il Gruppo di lavoro CODAU "Linee Guida Privacy e GDPR"

Il nuovo Regolamento UE 2016/679

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 (GDPR - General Data Protection Regulation o RGPD - Regolamento Generale sulla Protezione dei Dati)

- Abroga il Regolamento UE 95/46/CE
- Data entrata in vigore: **24 maggio 2016**
- Definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal **25 maggio 2018**
- Costituito da: 173 " Considerando ", XI Capi, 99 articoli
- Punti principali di attenzione:
  - Ruoli e responsabilità
  - Accountability, misure di sicurezza e analisi d'impatto
  - Diritti degli interessati: Informativa, Consenso, Diritti tradizionali

- Maggiori informazioni e linee guida sono disponibili sul sito del Garante, all'indirizzo : http://www.garanteprivacy.it/regolamentoue

I soggetti del trattamento

Il Titolare del trattamento
Persona fisica o giuridica che raccoglie i dati personali per proprie finalità e decide i mezzi per il trattamento

Il Contitolare del trattamento
Persona fisica o giuridica che condivide le finalità con altro Contitolare e stabilisce insieme a questi le modalità di trattamento

Il Responsabile del trattamento
Persona fisica o giuridica che esegue i trattamenti per conto del Titolare, sulla base di un contratto o di un atto giuridico. Può nominare **sub-responsabili**, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario, previa autorizzazione scritta, specifica o generale, del Titolare

Pur non prevedendo espressamente la figura dell' **"incaricato"** del trattamento, il regolamento **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"

I soggetti del trattamento: l'RPD

Designazione, obbligatoria per le PP.AA., di un "**Responsabile della protezione dei dati (RPD)**" (o, anche, "Data Protection Officer (DPO)"): è un soggetto interno o esterno all'Ente

Compiti dell'RPD:

- Agisce in autonomia e funge da collegamento fra Titolare/Responsabile, gli interessati e l'autorità di controllo;
- Informa e consiglia il titolare o il responsabile del trattamento, nonché i dipendenti, in merito all'applicazione del RGPD;
- Verifica l'attuazione e l'applicazione delle norme relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione degli incaricati, e gli audit relativi;
- Fornisce, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti.

Accresciuta responsabilità dei titolari e dei responsabili

La responsabilità dei titolari e dei responsabili si configura come una sostanziale assunzione di rischio, atteso che il titolare deve mettere in atto misure tecniche e organizzative adeguate per garantire la conformità del trattamento al Regolamento

- Il Regolamento promuove la responsabilizzazione (**accountability**) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.
- Il principio chiave è **"privacy by default and by design ". Attiene le buone prassi di protezione dei dati personali sin dalla progettazione del trattamento.**
- Il Titolare valuta **in autonomia** il rischio inerente al trattamento**,** senza preventiva autorizzazione e notifica all'autorità di controllo

Rafforzamento della qualità delle misure di sicurezza (1)

Sicurezza e valutazione dei rischi

La valutazione dei rischi e l'adozione di misure di sicurezza è rimessa, caso per caso, al Titolare e al Responsabile in rapporto ai rischi specificamente individuati

Misure di sicurezza

Tra le misure di sicurezza volte a garantire integrità, riservatezza e disponibilità di cui valutare l'adozione: la pseudonimizzazione, la cifratura, la resilienza dei sistemi e delle applicazioni, il loro tempestivo ripristino in caso di incidente

Valutazione d'impatto sulla protezione dei dati

Da effettuare per **i trattamenti con elevati rischi** (tecnologici, di finalità, di contesto, quali - ad esempio - i trattamenti connessi all'implementazione di trattamenti di profilazione o di sorveglianza, o all'introduzione di particolari tecnologie o all'utilizzo di particolari dati biometrici o giudiziari) per i diritti e le libertà delle persone fisiche, con redazione di un documento denominato **DPIA**

L'Autorità redige e pubblica l'elenco delle tipologie di trattamenti per le quali è richiesta una valutazione di impatto

Rafforzamento della qualità delle misure di sicurezza (2)

Registro delle operazioni di trattamento

La descrizione di tutti i trattamenti effettuati è riportata nel registro delle attività di trattamento tenuto da tutti i titolari e i responsabili di trattamento. Strumento indispensabile per ogni valutazione e analisi del rischio, deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante

Violazioni dei dati personali e relativa notifica

- Tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati
- Il responsabile informa il titolare senza ritardo in caso di violazioni
- Il titolare comunica una violazione dei dati personali all'interessato nei casi previsti dal Regolamento

Diritti degli interessati: Informativa

Contenuti obbligatori più estesi:

- Indicazione Responsabile Protezione Dati
- Tempi di conservazione dei dati
- Comunicazione a terzi
- Trattamenti automatizzati
- Diritti dell'interessato (es: a presentare reclami, alla portabilità)

Tempi:

- Prima della raccolta dei dati (se raccolti direttamente presso l'interessato)
- Nel caso di dati non raccolti direttamente presso l'interessato va fornita **entro 1 mese** dalla raccolta oppure, **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all'interessato)

Modalità:

- Formato elettronico
- Forma semplice, comprensibile e chiara
- Grafica standard

Diritti degli interessati: Consenso

Il consenso in generale deve essere: libero, specifico, informato e inequivocabile, non è ammesso il consenso tacito o presunto

Per gli enti pubblici, il consenso al trattamento dei dati personali non è necessario per i trattamenti connessi con le finalità istituzionali dell'ente

In generale, cambia poco rispetto alle previsioni del Codice (il d.lgs. 196/2003) salvo che:

- Non deve essere necessariamente documentato per iscritto
- Deve essere esplicito, manifesto e inequivocabile
- Non è ammesso il consenso tacito o presunto
- Il consenso dei minori è valido a partire dai 16 anni

Modalità:

- Formato elettronico
- Forma semplice, comprensibile e chiara

Diritti «tradizionali» degli interessati

Diritto di accesso:

- Risposta all'interessato entro 1 mese
- Copie dei dati con eventuale contributo per spese
- Idonea informativa con esplicitati i tempi di conservazione
- Auspicata la consultazione direttamente da remoto

Diritto di cancellazione (oblio):

- Il titolare deve estendere la richiesta anche ad altri titolari che trattano i dati cancellati
- Campo di applicazione più esteso dell'attuale

Diritto di limitazione del trattamento:

- Esercitabile non solo in caso di violazione di liceità
- Se è richiesta una rettifica dei dati
- Se l'interessato si oppone al trattamento, in attesa della valutazione del titolare

Diritto alla portabilità:

Linee-guida sul diritto alla portabilità dei dati - WP 242.pdf

Diritti «tradizionali» degli interessati

L’interessato ha il diritto di ricevere i dati personali forniti a un titolare, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmetterli a un altro titolare del trattamento senza impedimenti

La portabilità non sussiste (considerando 68 e l’art. 20, paragrafo 3, del RGPD) qualora il titolare agisca nell’esercizio di funzioni pubbliche. Ne deriva che un ente pubblico non è tenuto a prevedere procedure di portabilità. Tuttavia, è buona prassi mettere a punto meccanismi che consentano di rispondere in modo automatico a richieste di portabilità alla luce dei principi che disciplinano tale diritto

La portabilità non impone al titolare alcun obbligo di conservazione dei dati per un periodo superiore rispetto a quello eventualmente specificato

Il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall’interessato, se tecnicamente possibile

Diritto al risarcimento e responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento, ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Sanzioni amministrative

Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso effettive, proporzionate e dissuasive.

La violazione delle disposizioni del Regolamento è soggetta a **sanzioni amministrative pecuniarie fino a 20 000 000 EUR**, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.