Regolamento Europeo Privacy Cosa Cambia

Il nuovo Regolamento, insieme alla Direttiva in materia di trattamento e tutela dei dati personali costituisce il così detto **"Pacchetto protezione dati"**, che è stato approvato da parte del Parlamento dell'Unione Europea il 14 aprile del 2016.

Il Regolamento Europeo 679/2016, è da considerare un documento di indirizzo in quanto offre un quadro di riferimento in termini di "compliance" per la protezione dei dati in Europa, aggiornato e **fondato sul principio della responsabilizzazione ("accountability", secondo la terminologia anglosassone)** e troverà la sua applicazione direttamente per tutti gli Stati Membri a partire dal **25 maggio 2018.**

Il Regolamento Ue, sposta **la responsabilità di definire le misure di sicurezza idonee a garantire la sicurezza dei dati personali sul "titolare del trattamento".** Pertanto, nel quadro normativo delineato dal Regolamento Ue **non vi sono più delle misure minime di sicurezza stabilite "ex lege" ma solo delle misure di sicurezza che devono essere individuate e progettate dal "titolare del trattamento" o dal "responsabile del trattamento" ,** dopo avere condotto un'attenta analisi dei rischi (ed è proprio **l'analisi dei rischi,** condotta alla luce, anche, della tipologie e della rilevanza per l'interessato dei dati che dovranno essere sottoposti a trattamento, che diventa il momento centrale di tutto il processo)

Da ciò consegue che il **trattamento dei dati non può che avere inizio soltanto dopo la definizione delle misure di sicurezza** secondo uno schema operativo che va da:

- una **prima fase** costituita dalla definizione della tipologia di dati da sottoporre a trattamento,
- una **seconda fase** rappresentata dall'indicazione del tipo di trattamento cui sottoporli,
- una **terza fase**, in cui si provvederà alla verifica di quali possono essere i rischi di violazione della privacy dei dati nel corso del trattamento,
- una **quarta fase** in cui si dovrà passare all'identificazione delle opportune misure di sicurezza che dovranno essere prese.

definita dall'art. 25 Protezione dei Dati dalla progettazione e protezione per impostazione predefinita: Privacy by default e Privacy by design

Ove i trattamenti utilizzati dall'azienda siano forniti da soggetti terzi è compito del responsabile del trattamento provvedere a richiedere ed ottenere da tali soggetti terzi le appopriate valutazioni previste dal regolamento generale all'art. 25

Da un punto di **vista formale-organizzativo** il Nuovo Regolamento Europeo obbliga invece a ridefinire la parte documentativa del Decreto Legislativo n. 196/2003, ma **nella sostanza molti aspetti restano confermati**, anche se sotto forme diverse:

• il diritto all'oblio art. 17 (interessato ha diritto di ottenere la cancellazione dei suoi dati) da più parti punto ritenuto qualificante della nuova normativa, era in realtà già identificato attraverso la definizione dei diritti dell'interessato operata dal Codice;

• l'**informativa** sul trattamento dei dati personali conterrà le stesse informazioni che erano richieste dal Decreto Legislativo n. 196/2003;

• le modalità e la **liceità dei trattamenti e dei consensi** che l'interessato dovrà fornire al fine di rendere possibile il trattamento dei propri dati, comunque viaggerà sulle stesse logiche precedenti;

• **i registri dei trattamenti art. 30** erano già presenti nell'elenco dei trattamenti e nel Documento Programmatico di Sicurezza DPS . *Lo stesso deve essere inteso come un vero e proprio strumento di lavoro e come tale deve essere modificato e deve essere mantenuto aggiornato e sempre attuale.*

Un discorso diverso va fatto per:

- le **sanzioni**, che raggiungeranno il 4% del fatturato totale dei trasgressori o i 20 milioni di euro
- la **portabilità dei dati**, di cui all'articolo 20 del GDPR 16/679 (in base al quale ogni soggetto potrà chiedere ad un'organizzazione di ricevere i propri dati personali forniti in precedenza in un formato di uso comune e leggibile e di ottenerne la trasmissione da un titolare del trattamento a un altro se non sono presenti particolari impedimenti tecnologici,
- La **Responsabilità solidale** per le violazioni/sanzioni tra Titolare e Responsabile del Trattamento
- l'**istituzione del "Data Protection Officer**" (o DPO) ovvero il responsabile aziendale per la protezione dei dati **(solo ove necessario)**
- la **gestione dei "data breach" artt. 33 e 34** obbligo alla notifica all'Autorità di Controllo GARANTE quando c'è una violazione dei dati personali
- La **Valutazione di Impatto sulla protezione dei dati art. 35** è resa obbligatoria qualora il trattamento possa presentare un RISCHIO ELEVATO per i DIRITTI e le LIBERTA' delle Persone fisiche (art. 35 paragrafo 1 - 3 – 4) . Non essendo chiaro l'applicabilità in attività mediche/odontoiatriche di medie dimensioni il WP29 raccomanda di effettuarla comunque nel rispetto della normativa vigente

Al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla *protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'articolo 35, paragrafo 1 e all'articolo 35, paragrafo 3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e dei considerando 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che "possono presentare un rischio elevato"14,* ***si devono considerare i seguenti nove criteri.***

1. Valutazione o assegnazione di un punteggio, inclusiva di ***profilazione*** *e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;*

12 Cfr. considerando 71: "in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali". 13 Cfr. considerando 75: "se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza" . 14 Cfr. ad esempio i considerando 75, 76, 92 e 116.

*2. **processo decisionale automatizzato** che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;*

*3. **monitoraggio sistematico**: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c))15. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);*

*4. **dati sensibili o dati aventi carattere altamente personale**: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle **opinioni politiche** delle persone), nonché dati personali relativi a **condanne penali** o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;*

15 L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29 (cfr. le "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243): - che avviene per sistema; - predeterminato, organizzato o metodico; - che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; - svolto nell'ambito di una strategia. Il termine "zona accessibile al pubblico", a giudizio del WP29, indica qualsiasi luogo aperto a ciascun individuo della popolazione, come ad esempio una piazza, un centro commerciale, una strada, un mercato, una stazione ferroviaria o una biblioteca pubblica.

*5. **trattamento di dati su larga scala**: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala16: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento;*

*6. **creazione di corrispondenze o combinazione di insiemi di dati**, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato17;*

*7. **dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;*

*8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione **dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc.** Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;*

*9. quando il **trattamento in sé "impedisce agli interessati di esercitare un diritto** o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.*