PRIVACY (GDPR 679/2016)

Norme relative alla **protezione dei dati personali** => regolano e vincolano il loro trattamento
[Non si applica: in caso di trattamento da parte di persone fisiche per uso personale, se i dati sono trattati in modo non automatizzato e non sono destinati all'archiviazione, ai dati non di persone fisiche o resi anonimi]

Dati personali: informazioni riguardanti **persone fisiche** identificabili ("interessati")

dati comuni: anagrafici, relativi ai documenti, di contatto, bancari, auto, internet, di geolocalizzazione, di profilazione

dati particolari: relativi all'appartenenza a partiti, sindacati, religioni; dati genetici, biometrici, relativi alla salute (ex-sensibili)

dati giudiziari: relativi a condanne penali, reati e misure cautelari

Il loro **trattamento** – raccolta, organizzazione, conservazione, consultazione, trasmissione, distruzione – deve rispettare i seguenti **principi** (bisogna esser in grado di dimostrarlo: responsabilizzazione):

- Finalità: scopo del trattamento determinato, esplicito e legittimo
- Minimizzazione: dati adeguati, pertinenti e limitati a quelle finalità
- Esattezza: dati corretti e aggiornati
- Temporaneità: conservati per un arco di tempo limitato al conseguimento del fine
- Sicurezza: trattati con sistemi che garantiscano la loro adeguata protezione
- Trasparenza: nessun fine o trattamento deve essere nascosto all'interessato

Rispettati questi principi il trattamento è **lecito** solo se ricorre almeno una delle seguenti **basi giuridiche**:

- **Consenso:** l'interessato ha espresso il consenso per le finalità indicate
- **Contratto**: è necessario per l'esecuzione di impegni contrattuali dell'interessato
- **Obbligo**: è necessario per l'adempimento di un obbligo legale del titolare
- Rischi vitali: è necessario per la salvaguardia di interessi vitali dell'interessato
- Legittimo interesse: è necessario per perseguire il legittimo interesse del titolare o di terzi

Consenso Il titolare deve essere in grado di dimostrare che l'interessato ha manifestato la sua volontà al trattamento in modo libero, specifico, informato e inequivocabile. La richiesta deve essere chiara e comprensibile. Il consenso può essere revocato in qualsiasi momento. Non è lecito trattare dati di minori sotto i 16 anni senza il consenso dei genitori.

Dati particolari (art. 9) è vietato il loro trattamento a meno ché non sussista una delle seguenti condizioni, che si aggiunge alla base giuridica:

- il consenso esplicito a trattamento di questi dati per finalità specifiche;
- obblighi specifici del titolare o interessato in materia di diritto del lavoro, sicurezza e protezione sociale previsti dalla legge o dal CCNL e in presenza di garanzie appropriate
- trattamento effettuato da associazioni senza scopo di lucro (politiche, religiose, filosofiche, sindacali) dei dati degli associati/iscritti nell'ambito delle loro legittime attività
- trattamento necessario per finalità di medicina preventiva o del lavoro (valutazione dipendente)
- altri casi (interesse pubblico, interesse vitale, dati pubblici…)

I dati giudiziari, relativi a condanne penali e misure di sicurezza non possono essere trattati se non sotto il controllo dell'autorità pubblica.

Diritti dell'interessato

(art. 12-23)

Nel rispetto del principio di trasparenza l'interessato deve ricevere dal titolare, al momento della raccolta, tutte le **informazioni** relative ai dati e al loro trattamento, in forma concisa, trasparente, comprensibile con linguaggio semplice e chiaro (art.13):

1. identità e contatto del titolare del trattamento
2. contatto del DPO (eventuale)
3. finalità del trattamento
4. legittimi interessi perseguiti se questi sono la base giuridica (eventuale)
5. destinatari esterni a cui sono comunicati coerentemente con le finalità indicate (eventuale)
6. intenzione di trasferirli ad un paese terzo extra UE o organizzazione internazionale (eventuale)
7. periodo di conservazione in relazione alle finalità indicate
8. esistenza del diritto di accesso, rettifica, cancellazione, di limitazione del trattamento, di opposizione, di portabilità
9. esistenza del diritto di revoca del consenso (eventuale)
10. esistenza del diritto di proporre reclamo ad un'autorità di controllo
11. se la comunicazione è un obbligo di legge o contrattuale nonché le possibili conseguenze di un rifiuto: preclude l'esecuzione del ctr o l'assolvimento degli obblighi (no se dati non ottenuti dall'interessato)
12. esistenza di un processo decisionale automatizzato compresa la profilazione (occorre consenso esplicito)

Se i dati sono ottenuti non presso l'interessato, le informazioni di cui sopra sono fornite in tempi ragionevoli insieme alle seguenti (art. 14):

13. le categorie dei dati personali trattati
14. la fonte da cui hanno origine i dati personali

Oltre ad essere informato l'interessato ha tutti i **diritti** di seguito elencati e il titolare deve agevolare il loro esercizio e soddisfare le sue richieste senza ingiustificato ritardo, al più tardi entro un mese:

Diritto di accesso (art.. 15) ai dati e alle informazioni sul trattamento

Diritto di rettifica (art. 16) di dati inesatti o incompleti

Diritto di cancellazione (art. 17) dei dati che lo riguardano (oblio)

Diritto di limitazione (art. 18) del trattamento nelle ipotesi previste

Diritto alla portabilità (art. 20) dei dati ottenuti in formato strutturato e leggibile

Diritto di opposizione (art. 21) al trattamento dei dati che lo riguardano nei casi specifici (base giuridica rappresentata da interesse pubblico o legittimo interesse del titolare)

Diritto di non essere sottoposto a processo decisionale automatizzato (art. 22) compresa la profilazione.

Organigramma Privacy

Titolare
(data controller)

il titolare del trattamento è il soggetto, persona fisica o giuridica, che determina le finalità e i mezzi del trattamento e ne è responsabile. Tenuto conto dell'ambito di applicazione, delle finalità e dei rischi per i diritti delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Riesamina e aggiorna tali misure qualora necessario.

RPD/DPO

responsabile della protezione dei dati (data protection officer), soggetto interno o esterno, che in piena indipendenza supporta il titolare nell'applicazione del regolamento e funge da punto di contatto per le questioni in tema di privacy. Verifica la regolarità dei processi e va coinvolto nella organizzazione del trattamento dei dati. Ha funzioni di supporto, controllo, consultive, formative e informative.
Deve avere una buona padronanza della normativa, esperienza in materia di organizzazione, procedure informatiche e sicurezza e deve conoscere la realtà operativa in cui avvengono i trattamenti.
E' nominato con atto scritto di designazione, se interno, o con contratto di servizi se esterno. Gli atti devono indicare espressamente i compiti attribuiti e le risorse assegnate (finanziarie, infrastrutture, personale se necessario). Il suo nominativo va comunicato al Garante e i dati di contatto pubblicati dal titolare.
E' obbligatorio solo nel caso in cui il trattamento è effettuato su larga scala in termini di interessati o di categorie particolari di dati.

Responsabile
(data processor)

il responsabile del trattamento e il soggetto esterno alla struttura del titolare che tratta i dati per suo conto. Deve essere in grado di attuare le adeguate misure tecniche ed organizzative per il rispetto del Regolamento. Il rapporto è disciplinato da un contratto. Può ricorrere ad un sub-responsabile se autorizzato dal titolare (art. 28 - C. 81).
Non tutti i soggetti che forniscono servizi al titolare del trattamento sono responsabili, lo sono solo se trattano i dati per conto e su istruzioni di questo. Nel caso in cui hanno il controllo sulla tipologia di dati, finalità e modalità del trattamento allora sono essi stessi titolari (data controller). In genere le banche, gli avvocati, i medici.

Incaricati

soggetti che trattano i dati sotto l'autorità del titolare o del responsabile. Devono essere autorizzati e istruiti da questi sulle modalità e rischi del trattamento. Vale il principio della minimizzazione. Non esplicitamente previsti dal Regolamento (ex art. 30 Codice).

Referente privacy

figura facoltativa delegata dal titolare per fini organizzativi agli adempimenti in materia di privacy, potrebbe sostituire il vecchio responsabile interno, ma non libera il titolare che rimane l'unico soggetto che deve provare il rispetto del regolamento.

Organizzazione trattamento dati

Il Titolare del trattamento deve metter in atto **misure tecniche ed organizzative adeguate** a garantire il rispetto del regolamento e dei diritti degli interessati.

Il rispetto della privacy deve essere previsto nella progettazione dell'organizzazione e dei processi aziendali (privacy by design) prevedendo anche che per default vengano trattati solo i dati necessari per ogni specifica finalità limitando il numero di persone fisiche che avranno accesso ai dati (privacy by default).

Tra le possibili misure da adottare, anche in ottica di maggiore sicurezza, vi sono:
- la pseudonimizzazione e la cifratura, procedure per rendere anonimi i dati senza l'utilizzo di informazioni aggiuntive che devono essere conservate separatamente;
- la minimizzazione dei dati trattati, limitati al necessario rispetto alle finalità perseguite;
- la trasparenza con gli interessati sui dati trattati;
- la capacità di assicurare permanentemente la riservatezza e l'integrità dei dati e di ripristinare tempestivamente la disponibilità e l'acceso in caso di incidente;
- la predisposizione di una procedura per testare e valutare l'efficacia delle misure volte a garantire la sicurezza dei dati.

Le misure tecniche ed organizzative devono essere definite tenendo conto oltre che della natura e delle finalità del trattamento anche dei **rischi esistenti**, con probabilità e gravità diverse, per i diritti e le liberta degli interessati. Tali rischi sono relativi al trattamento di dati suscettibili di cagionare un danno fisico, materiale o immateriale: furto o usurpazione di identità, perdite finanziarie, danno alla reputazione, perdita di riservatezza di dati protetti da segreto professionale, altri danni significativi.

Il titolare, con la consulenza del DPO, dovrà quindi individuare il rischio connesso al trattamento, valutarlo in termini di origine, natura, gravità e probabilità e definire le adeguate misure per attenuarlo anche attraverso una **policy interna**. Tali misure potrebbero derivare da codici di condotta o linee guida del Garante o da certificazioni approvate.

Registro delle attività di trattamento

Fornisce un quadro riepilogativo delle operazioni di trattamento dei dati in essere. Deve avere forma scritta ed essere esibito su richiesta del garante. Obbligatorio se più di 250 dipendenti.

- Nome e contatto Titolare e DPO
- Finalità trattamento
- Categorie di interessati e categoria di dati trattati
- Categorie di destinatari
- Trasferimento a paresi terzi extra UE (eventuale)
- Termini previsti per la cancellazione
- Descrizione misure di sicurezza adottate