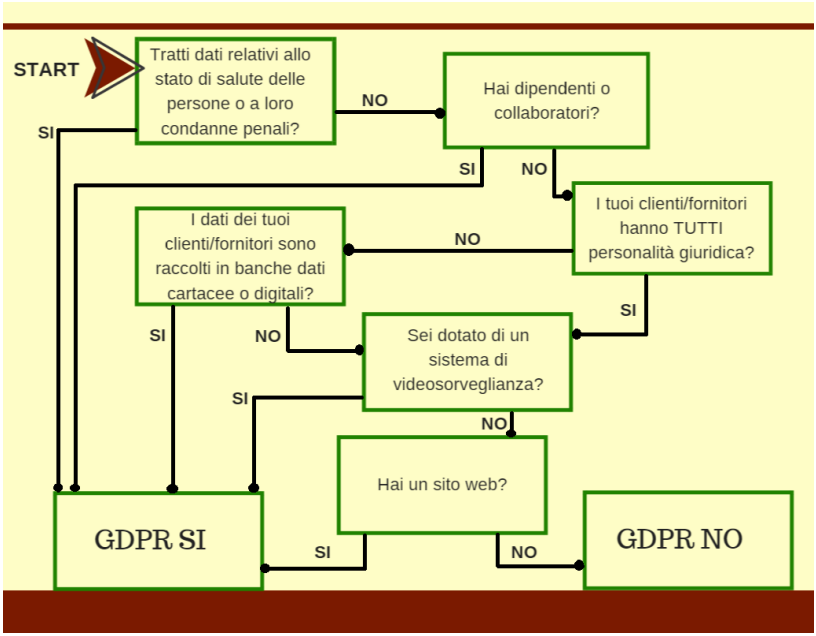
I quaderni di Aesse Servizi

La protezione dei dati personali secondo il

GDPR 2016/679

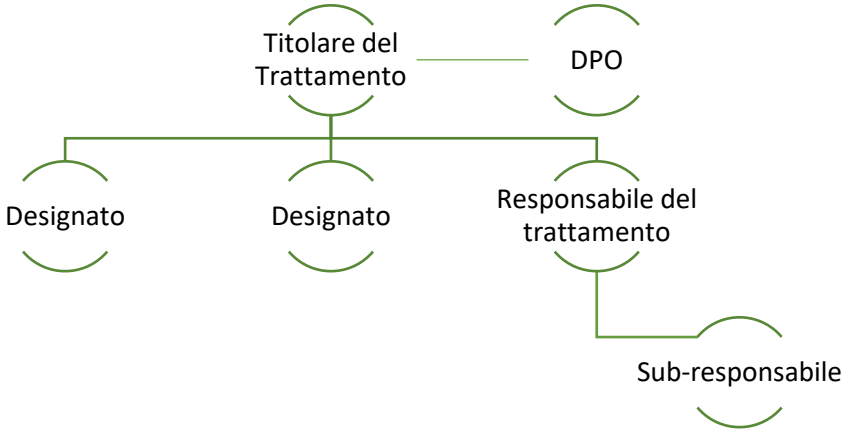
A chi si applica?



Inoltre, il GDPR NON si applica se:

- Il trattamento ha carattere domestico o personale;
- Il trattamento è effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Organigramma privacy



Il Titolare del trattamento

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina finalità e mezzi del trattamento dei dati personali.

Esso detiene, quindi, il potere decisionale in ordine al trattamento.

Il titolare deve precostituire:

- Un apparato DOCUMENTALE idoneo a garantire la protezione dai rischi dal punto di vista formale;
- Un apparato di misure FISICHE E ORGANIZZATIVE che proteggano effettivamente gli individui e i loro dati.

Il Responsabile del trattamento

È la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare.

Il rapporto tra Titolare e Responsabile è sempre disciplinato da un contratto o altro atto a norma del diritto dell'UE o degli Stati membri.

Ha facoltà di nominare dei sub-responsabili, ma in caso di inadempienza da parte del sub-responsabile, il responsabile conserva le responsabilità iniziali nei confronti del Titolare.

I soggetti designati

Sono le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Nel regolamento UE non vi è una definizione espressa.

Il Titolare ha l'obbligo nei confronti dei soggetti designati di:

- Consegna delle istruzioni scritte e di tutti i disciplinari presenti;
- Formazione.

Il Responsabile della Protezione Dati

È obbligatoria la nomina del DPO:

- Per le autorità o gli organismi pubblici;
- In caso di monitoraggio regolare e sistematico degli interessati su larga scala;
- In caso di trattamento su larga scala di categorie particolari di dati personali (art. 9) o di dati relativi a condanne penali e a reati (art. 10).

…fermo restando che il DPO può sempre essere facoltativamente nominato!

Può trattarsi di un dipendente del titolare o del responsabile oppure un soggetto esterno legato al titolare/responsabile da un contratto di servizi, purché:

- Non si trovi in conflitto di interesse;
- Abbia conoscenza specialistica della normativa e delle pratiche in materia di protezione dati.

Privacy by design e by default

Prevenire, non correggere

- è preferibile adottare misure di sicurezza adeguate a prevenire eventuali danni, piuttosto che correre ai ripari dopo

Privacy come impostazione di default

- ogni sistema IT utilizzato deve già includere tutte le impostazioni privacy necessarie a garantire la sicurezza del trattamento

Privacy incorporata nella progettazione

- la privacy deve essere inclusa e integrata fin dall'inizio in ogni progetto

Massima funzionalità di protezione dei dati

- la privacy deve essere considerata come un valore aggiunto

Sicurezza durante tutto il ciclo del trattamento

- la sicurezza del trattamento deve essere garantita durante l'intero processo

Trasparenza delle informazioni all'interessato

- il linguaggio utilizzato nelle ifnormative deve essere chiaro e attagliato all'età dell'interessato

Trattamento User Centric

- l'operatore deve sempre avere un ruolo centrale nel trattamento

Inoltre…

Privacy by default

- Principio di minimizzazione dei dati
- Conservazione dei dati fino al raggiungimento dello scopo

Basi di liceità del trattamento

- CONTRATTO
- LEGGE
- INTERESSE PUBBLICO
- INTERESSE VITALE
- INTERESSE LEGITTIMO DEL TITOLARE
- CONSENSO

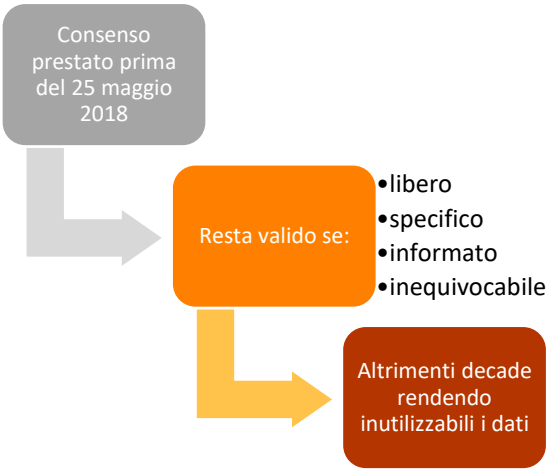
Ogni trattamento deve poggiarsi su una delle sei basi di liceità citate.

Consenso

Deve essere:

- Libero, specifico, informato e inequivocabile: non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo);
- Manifestato attraverso "dichiarazione o azione positiva inequivocabile";
- Distinguibile da altre richieste/dichiarazioni;
- Esplicito per i dati particolari e per le decisioni basate su trattamenti automatizzati.

Non deve essere necessariamente in "forma scritta", ma il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.



Informativa

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del GDPR, ampliando in parte quando richiesto dal Codice privacy. In particolare, devono essere specificati

- I dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente;
- La base giuridica del trattamento;
- Se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.

Inoltre il titolare deve chiarire

- Il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- Il diritto di presentare un reclamo all'autorità di controllo;
- Se il trattamento comporta processi decisionali automatizzati (anche la profilazione) e, in caso affermativo, la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Registri dei trattamenti

Casi di obbligatorietà:

- Società con più di 250 dipendenti;
- Si svolgono trattamenti che recano rischi per la privacy:
    - Il trattamento svolto NON è occasionale;
    - Si trattano dati particolari o giudiziari.

La sicurezza del trattamento (art.32)

“Il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) La pseudonimizzazione e la cifratura dei dati personali;
b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.”

Data Breach

La notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare.

Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

Sanzioni amministrative

Fino a...	e per le imprese...
10 milioni	fino al 2% del fatturato mondiale totale annuo, dell'esercizio precedente se superiore
20 milioni	fino al 4% del fatturato mondiale totale annuo, dell'esercizio precedente se superiore

Il soggetto designato

……

con mansione di ……

DICHIARA

di aver ricevuto copia de "I quaderni di Aesse Servizi – La protezione dei dati personali secondo il GDPR 2016/679".

Luogo e data……..

Firma……