IL TITOLARE DEL TRATTAMENTO, IL CONTITOLARE E IL RESPONSABILE DEL TRATTAMENTO NELLA PROTEZIONE DEI DATI PERSONALI

BREVI CENNI AI LORO OBBLIGHI E ALLE DOMANDE DA PORSI PER UNA CORRETTA GESTIONE DEI DATI PERSONALI PRIMA DI INIZIARE LE ATTIVITÀ DI TRATTAMENTO

Sommario

PREMESSA[1]

Il **Regolamento europeo 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE** (GDPR) individua espressamente le diverse figure che operano nell'ambito del trattamento dei dati personali con ruoli e responsabilità diversificate. Esse sinteticamente sono:

1. **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 le finalità e i mezzi del trattamento di i dati personali.
   Nel caso due o più titolari decidano congiuntamente i le finalità e i mezzi del trattamento si parla di **contitolarità.** Tale rapporto può assumere varie forme e la partecipazione dei diversi titolari del trattamento alle varie attività può differire. Il Gruppo di lavoro articolo 29 nel suo parere del 2010 afferma che i contitolari del trattamento possono condividere tutte le finalità e tutti gli strumenti di un trattamento, alcune finalità o mezzi o una parte di essi. Nel primo caso la relazione tra i diversi attori sarebbe molto stretta nel secondo più distante.
   In ogni caso i contitolari devono disciplinare i loro rapporti mediante un accordo interno stabilendo le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del Regolamento 2016/679;
2. **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 del trattamento.
   Le attività di trattamento affidate ad un responsabile del trattamento possono essere limitate a un compito o a un contesto specifico o possono essere molto generali. Essenziale nel rapporto tra titolare e responsabile del trattamento è il contratto o altro atto giuridico che viene stipulato tra i due.
   Si tratta di un atto giuridicamente obbligatorio che deve disciplinare la materia e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.
   I Responsabili del trattamento agiranno in qualità di titolare autonomo quando tratteranno dati per proprio conto (ad esempio i dati dei propri dipendenti, la tenuta della contabilità ecc.).

Di seguito sono riportate:

- alcune indicazioni di massima relativamente agli obblighi in capo alle due figure sopra citate per il rispetto della normativa europea in materia di protezione dati;
- alcune informazioni circa il contenuto che deve avere un atto/contratto di nomina a responsabile del trattamento;
- un diagramma di flusso utile per capire qual è il proprio ruolo quando si trattano dati con terze parti;
- alcune domande che un soggetto dovrebbe porsi prima di iniziare qualsiasi operazione di trattamento per il corretto.

Per maggiori informazioni e facsimili è possibile consultare la sezione intranet di Ateneo Protezione Dati – Privacy (https://www.unifi.it/p11551.html).

[1] Nel predisporre il documento si si è fatto riferimento alla pubblicazione del Garante europeo per la protezione dati Flowcharts and Checklists on Data Protection – Brochure e al Manuale sul diritto europeo in materia di protezione dati – edizione 2018 FRA/Corte EDU/GEPD

Quali sono i doveri del Titolare del Trattamento?

Il trattamento dei dati personali deve rispettare i seguenti principi:

- deve essere lecito, giusto e trasparente (liceità, equità, trasparenza);
- deve essere vincolato a finalità specifiche (limitazione delle finalità);
- i dati personali trattati dovrebbero essere adeguati, pertinenti e limitati a quanto necessario (minimizzazione dei dati);
- i dati personali devono essere esatti (esattezza);
- i dati personali non devono essere conservati più a lungo del necessario (limitazione della conservazione);
- i dati personali devono rimanere ben protetti e riservati (integrità e riservatezza).

Il Titolare del Trattamento è responsabile della conformità a questi principi delle operazioni di trattamento dati da lui operate e dovrebbe essere in grado di dimostrare tale conformità (principio di accountability). A tal fine, i titolari del trattamento in pratica devono:

- documentare le loro operazioni di trattamento con la tenuta del Registro attività di trattamento (art. 30 GDPR);
- effettuare, se necessario, una valutazione d'impatto sulla protezione dei dati (DPIA) prima delle operazioni che comportano un rischio elevato per i diritti e le libertà delle persone interessate;
- in determinate circostanze, consultare il Garante per la protezione dei dati personali prima di iniziare attività di trattamento ad alto rischio;
- nella progettazione delle operazioni di trattamento, tenere presenti i principi di privacy by design e privacy by default;
- adottare adeguate misure di sicurezza per proteggere i dati personali;
- in caso di violazione di dati personali informare, se necessario, il Garante per la protezione dei dati personali e, in determinate circostanze, le persone interessate;
- concludere accordi/contratti solo con i Responsabili del trattamento che forniscono garanzie adeguate di sicurezza e riservatezza;
- concludere accordi con altri titolari in caso di contitolarità per disciplinare i rispettivi obblighi e doveri;
- trasferire dati personali, verso altri paesi dell'UE, verso paesi non appartenenti all'UE o organizzazioni internazionali solo se sono rispettate le condizioni del GDPR;
- cooperante con il Garante per la protezione dei dati personali.

Infine, il titolare del trattamento deve fornire alle persone interessate informazioni chiare e accessibili sul trattamento, rispettare e garantire i diritti delle persone interessate.

Quali sono i doveri del Responsabile del trattamento

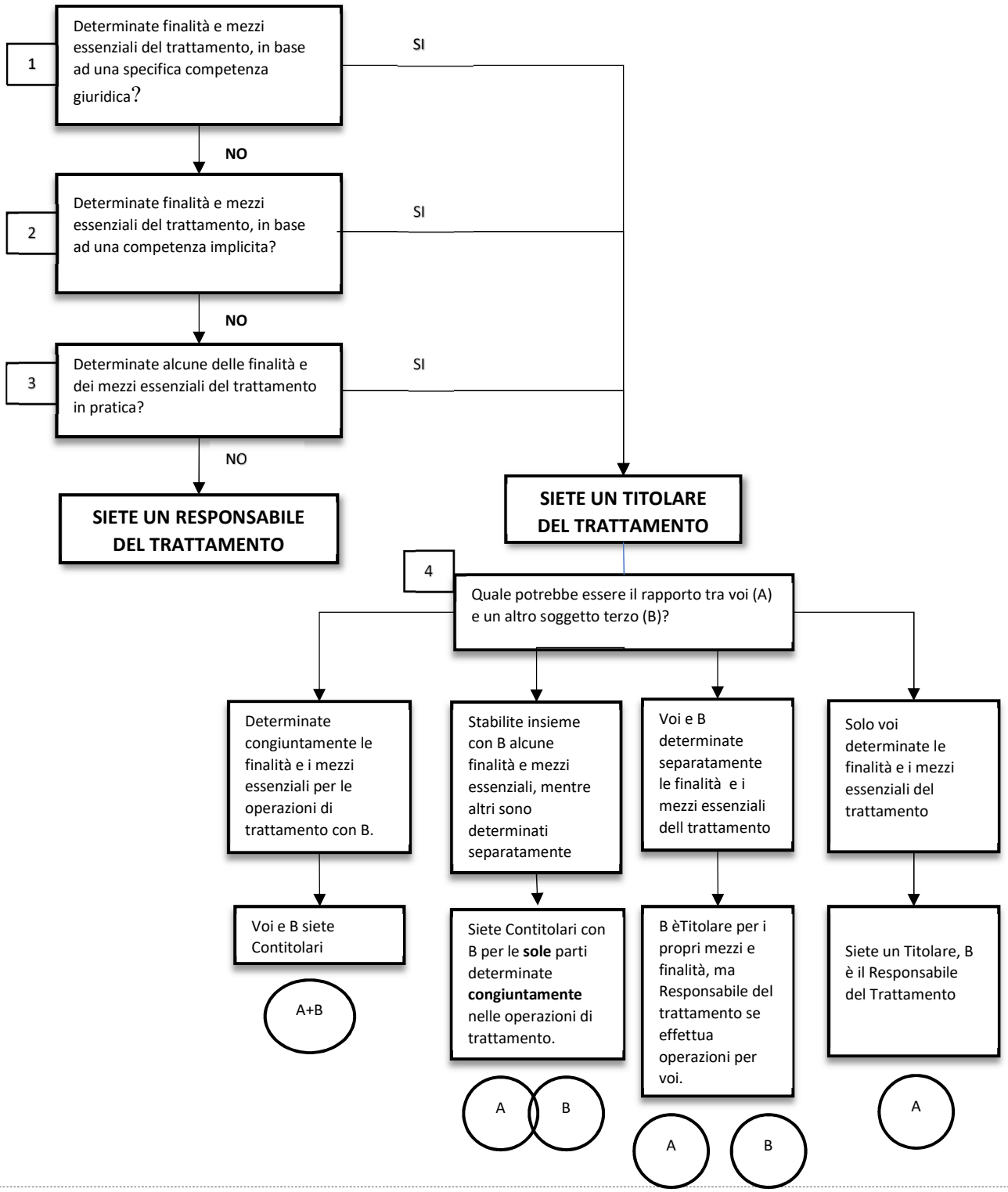
Per conformarsi al Regolamento UE 2016/679 i Responsabili del trattamento devono:

- trattare i dati personali solo su istruzioni documentate del titolare del trattamento, a meno che ciò non sia richiesto dal diritto dell'UE o degli Stati membri;
- trattare i dati personali come stabilito in un contratto o un altro atto giuridico vincolante e che stabilisce i presupposti necessari per svolgere tale compito;
- NON trattare ulteriormente i dati per altri scopi incompatibili;
- assistere il titolare del trattamento per garantire i diritti degli interessati e di adempiere agli obblighi normativi previsti dal GDPR;
- notificare qualsiasi richiesta giuridicamente vincolante di divulgazione dei dati personali trattati per conto del titolare del trattamento e dare accesso ai dati solo previa autorizzazione scritta del titolare del trattamento;
- esternalizzare/subappaltare a sub-referenti le attività di trattamento SOLO con la preventiva autorizzazione scritta del titolare del trattamento;
- informare successivamente il titolare del trattamento di eventuali variazioni sui contratti stipulati con i sub-referenti, dando al medesimo la possibilità di opporsi alle modifiche; trasmettere gli stessi obblighi contrattuali a eventuali subappaltatori;
- tenere un registro delle attività di trattamento svolte per conto del titolare del trattamento;
- adottare adeguate misure di sicurezza per proteggere i dati personali;
- informare senza indebito ritardo il Titolare del trattamento della violazione dei dati;
- cooperare, su richiesta, con il Garante per la protezione dei dati personali nell'esecuzione dei suoi compiti.

SIETE UN RESPONSABILE, UN TITOLARE DEL TRATTAMENTO O UN CONTITOLARE?

Siete coinvolti in un'operazione di trattamento con una o più terze parti: Siete un Responsabile, un Titolare o un Contitolare?

! **Questo diagramma di flusso riguarda le situazioni in cui l'attribuzione dei ruoli di Responsabile e/o di Titolare del trattamento non è stata stabilita espressamente in una norma o regolamento**



Che cosa è richiesto in un contratto o da altro atto giuridico di nomina a responsabile del trattamento ai sensi dell'art. 28 del GDPR?

I Titolari del trattamento possono chiedere a un soggetto terzo di trattare dati personali per loro conto.

Il trattamento esternalizzato riguarda quindi dati personali prodotti ed elaborati così come previsto nel contratto/altro atto giuridico, non i dati del contraente o del suo personale.

Il trattamento dei dati da parte di un Responsabile richiede un contratto o un altro atto giuridico vincolante ai sensi del diritto dell'UE o degli Stati membri, che disciplini:

- finalità, durata, natura e portata del trattamento;
- tipo di dati personali e le categorie di interessati;
- periodo di conservazione dei dati;
- ubicazione dei dati e accesso ai dati (sulla base di una valutazione preliminare dei rischi può essere limitato o meno al SEE);
- destinatari dei dati e trasferimenti di dati;
- misure di sicurezza (che garantiscano almeno lo stesso livello di sicurezza dei dati personali assicurato dal titolare del trattamento);
- che il responsabile del trattamento può agire solo su istruzioni documentate del titolare del trattamento, a meno che ciò non sia richiesto dalla legislazione dell'UE o degli Stati membri Deve contenere istruzioni anche sul trasferimento di dati personali e sull'assistenza al titolare del trattamento;
- eventuali leggi aggiuntive sulla protezione dei dati (ad es. direttiva e-privacy, direttiva NSI) - se applicabili;
- il ricorso a sub-responsabili solo con precedente autorizzazione scritta del controllore e le comunicazioni di eventuali modifiche in debito anticipo;
- le misure di riservatezza e l'accesso ai dati solo alle persone autorizzate sulla base della necessità di conoscere;
- i diritti di controllo del titolare del trattamento sui responsabili del trattamento e sui sub-responsabili;
- la cooperazione, su richiesta, con il Garante per la protezione dei dati personali nell'esecuzione dei suoi compiti;
- la divisione dei compiti tra contitolari - se del caso - in modo che il Responsabile sappia come assistere il singolo contitolare;
- l'assistenza per le richieste di diritti dell'interessato;
- l'assistenza nell'adempimento degli obblighi del titolare del trattamento (notifica della violazione della sicurezza e dei dati, valutazione dell'impatto sulla protezione dei dati e consultazione preventiva, riservatezza delle comunicazioni elettroniche, ecc.) e tenuta del registro delle attività di trattamento per conto del titolare del trattamento,
- l'assistenza in caso di violazione dei dati;
- la scelta da parte del titolare del trattamento di farsi restituire o far cancellare i dati dal Responsabile al termine del trattamento;
- l'obbligo di informare il Titolare se le sue istruzioni violano il GDPR o altre disposizioni dell'UE o dello Stato membro in materia di protezione dei dati;
- i motivi di risoluzione in caso di grave inadempienza del responsabile del trattamento, responsabilità, ecc.;

- altre disposizioni eventualmente applicabili che riguardano la protezione dei dati (ad esempio la legge e la giurisdizione applicabili in caso di Responsabili del trattamento esteri, ecc.).

Domande da porsi prima di intraprendere operazioni di trattamento di dati personali.

ALCUNE DOMANDE DA PORSI NELLE OPERAZIONI DI TRATTAMENTO PER GARANTIRE I PRINCIPI DI CUI ALL'ARTICOLO 5 DEL GDPR	
Trasparenza delle informazioni	– Come informerete le persone dei vostri trattamenti? – Come vi assicurate che le informazioni raggiungano le persone interessate? – Avete fornito tutte le informazioni necessarie? Sono facilmente comprensibili? – Il linguaggio utilizzato per fornire informazioni è adatto per la tipologia di interessati? (ad esempio i bambini, ecc.) – Nel caso in cui si rinvia il momento per fornire le informazioni, qual è la vostra giustificazione?
Correttezza	– Che cosa si aspettano le persone dalle attività di trattamento dati, anche se non leggono le informazioni fornite loro? – In caso di affidamento sul consenso, esso è davvero libero? Come si fa a documentare che le persone lo hanno dato? Come possono revocare il loro consenso? – Il trattamento dei dati potrebbe generare effetti negativi sugli interessati? – Il trattamento dei dati potrebbe condurre a discriminazioni degli interessati? – È facile per le persone esercitare i loro diritti di accesso, rettifica, ecc?
Limitazione delle finalità	– Avete identificato tutte le finalità del trattamento dei dati? – Tutte le finalità sono compatibili con quella iniziale? – C'è il rischio che i dati possano essere riutilizzati per altri scopi? – Come si può garantire che i dati vengono utilizzati solo per le loro finalità definite? – Se si desidera rendere disponibili/riutilizzare i dati per la ricerca scientifica, a fini statistici o storici, quali garanzie si applicano per proteggere gli individui interessati?
Minimizzazione dei dati	– I dati sono di qualità sufficiente per la finalità perseguite? – I dati raccolti misurano ciò che si intende determinare? – Ci sono alcune tipologie di dati che potrebbero essere rimossi senza compromettere lo scopo del processo? – Nei moduli utilizzati nei trattamenti sono distinti chiaramente gli elementi obbligatori da quelli opzionali? – Nel caso in cui si desideri conservare le informazioni a fini statistici, come si gestisce il rischio di re-identificazione?

Esattezza	– Quali potrebbero essere le conseguenze per le persone interessate agendo su informazioni inesatte durante le operazioni di trattamento? – Come si fa a garantire che i dati che si raccolgono siano esatti? – Come garantire che i dati ottenuti da terze parti siano esatti? – Gli strumenti utilizzati nelle operazioni di trattamento consentono aggiornamenti/correzioni dei dati laddove necessario? – Gli strumenti utilizzati nelle operazioni di trattamento consentono controlli di coerenza?
Limitazione della conservazione	– Esiste una norma che definisce i periodi di conservazione per i dati oggetto del trattamento? – Per quanto tempo è necessario conservare i dati? Per quale finalità? – Potete distinguere periodi di archiviazione per le diverse tipologie dei dati? – Se non è ancora possibile eliminare i dati, è possibile limitare l'accesso ad essi? – Gli strumenti utilizzati per conservare i dati consentono la cancellazione automatica alla fine del periodo di archiviazione?
Sicurezza	– Disponete di una procedura per l'identificazione, l'analisi e la valutazione dei rischi per la sicurezza delle informazioni che potrebbero riguardare i dati personali e i sistemi informatici a supporto del loro trattamento? – Avete tenuto conto dell'impatto delle operazioni di trattamento sui diritti, le libertà e gli interessi fondamentali delle persone e non solo i rischi per l'organizzazione? – Prendete in considerazione la natura, la portata, il contesto e le finalità del trattamento al momento della valutazione dei rischi? – Gestite le vulnerabilità di sistema e le minacce per i vostri dati e sistemi? – Avete risorse o personale con ruoli assegnati per eseguire delle valutazioni del rischio?

ALTRE DOMANDE UTILI DA PORSI

Quali fattori devo tenere in considerazione in sede di pubblicazione dei dati personali

- Sono obbligato a pubblicare? Posso pubblicare? (Base giuridica)
- Cosa posso pubblicare? (Minimizzazione dei dati)
- Come faccio a informare gli individui interessati? (Informazioni)
- Come mi assicuro che i dati sono corretti? (Accuratezza)

Perché informare le persone sul trattamento dei dati?

In modo che possano:

- capire quali dei loro dati sono trattati e come;
- verificare la qualità dei propri dati;
- esercitare gli altri diritti di in materia di protezione dei dati (accesso, rettifica, cancellazione, limitazione del trattamento, notifica di rettifica, limitazione del trattamento, portabilità dei dati, opposizione, non essere oggetto di una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione).

In sintesi alcuni consigli

➢ *Pensate a cosa dovete fare per soddisfare le vostre finalità e limitatevi ai trattamenti necessari per raggiungerle.*
➢ *Definite quello che fate e documentatelo.*
➢ *Informate le persone e rispettate i loro diritti in materia di protezione dati*