Disciplina dei rapporti tra Titolare del Trattamento(ARSIAL) e Responsabile (esterno) del Trattamento in conformità al GDPR.

Definizioni

Il **Titolare del trattamento** nel GDPR è definito all'art. 4, par. 1, n. 7) come «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» *(Data controller)*

Il **Responsabile del trattamento** nel GDPR è definito all'art. 4, par. 1, n. 8) come "la persona fisica, giuridica, PA o ente che tratta i dati personali per conto del titolare del trattamento". *(Data processor). Necessità di un accordo*

I **Contitolari del trattamento** sono invece definiti all'art. 26 del GDPR nel modo seguente: «Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento,….. » *Necessità di un accordo*

L'art. 28 del GDPR

1. **Qualora un trattamento vada effettuato per conto del titolare** del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. I**l responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta,** specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. **I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata 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.**

L'art. 28 del GDPR

Il c**ontratto o altro atto giuridico prevede, in particolare,** che il responsabile del trattamento:

a) tratti i dati personali soltanto su **istruzione documentata** del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le **persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza**;

c) adotti tutte le **misure richieste ai sensi dell'articolo 32**;

d) rispetti le condizioni di cui ai **paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento**;

e) tenendo conto della natura del trattamento, **assista il titolare del trattamento con misure tecniche e organizzative adeguate,** nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

L'art. 28 del GDPR

f) **assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, t**enendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su **scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi** relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) **metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi** di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla l**ettera h)** del primo comma, il responsabile del trattamento **informa immediatamente il titolare** del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla
protezione dei dati.

L'art. 28 del GDPR

4. Q**uando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento,** su tale altro responsabile del trattamento sono imposti, **mediante un contratto o un altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo

L'art. 28 del GDPR

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.
7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.
9. **Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.**
10. **Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.**

L'art.30 del GDPR

Il Responsabile deve tenere un registro dei trattamenti:

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

L'art. 33 del GDPR

In caso di **Data Breach (violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati).**

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione

(art. 33 comma 2)

E' opportuno disciplinare nell'accordo questo aspetto, assegnando eventualmente un termine al Responsabile del trattamento per effettuare le comunicazioni al Titolare, in modo che quest'ultimo possa effettuare la comunicazione nel termine previsto dalla norma di 72 ore dal momento in cui ne è venuto a conoscenza.

Il Regolamento UE fissa dettagliatamente le caratteristiche dell'atto con cui il Titolare designa un responsabile del trattamento, attribuendogli specifici compiti:

-deve trattarsi, infatti, di un **contratto (o altro atto giuridico** conforme al diritto nazionale- ad esempio, addendum contrattuale)

-deve disciplinare tassativamente almeno le materie riportate al par. 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "**garanzie sufficienti**", quali, in particolare:

- l**a natura, durata e finalità del trattamento o dei trattamenti assegnati,**
- **le categorie di dati oggetto di trattamento,**
- **le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento;**

Il Regolamento UE:

consente la **nomina di sub-responsabili** del trattamento da parte di un responsabile (art. 28, par. 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario;

Il Responsabile del Trattamento **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (art. 82, par. 1, e par. 3);

Il Regolamento:

prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari.

Ciò riguarda, in particolare,

- la tenuta del **registro dei trattamenti** svolti (art. 30, par. 2);
- l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (art. 32);
- **la designazione di un RPD-DPO** (si segnalano, al riguardo, le Linee guida sui responsabili della protezione dei dati, adottate dal Gruppo "Articolo 29"), nei casi previsti dal Regolamento o dal diritto nazionale (art. 37).

Le Linee Guida dell'EDPB n. 7/2020

Le Linee guida **dell'European Data Protection Board** (EDPB) o **Comitato Europeo per la Protezione dei Dati**, hanno lo scopo di dirimere i dubbi relativi alla corretta definizione dei concetti di titolare e responsabile e i rispettivi ruoli, rispetto alle quali da tempo si avvertiva la necessità di un chiarimento autorevole.

Tra queste rilevano, in particolare, le specifiche obbligazioni e i vincoli imposti dall'art. 28 GDPR al responsabile del trattamento nei confronti del titolare.

Condizioni indispensabili per configurare il ruolo di Responsabile del trattamento

1) essere un **soggetto distinto** rispetto al titolare del trattamento
2) e trattare dati personali **per conto** del titolare del trattamento.

- I soggetti (persone fisiche, giuridiche, P.A.) **che trattano dati personali** per conto del titolare **devono essere designate responsabili del trattamento**.

- Responsabile del trattamento non può essere chiunque, ma solo chi può offrire **garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate**

- Il rapporto tra titolare e responsabile deve essere regolato da un **contratto o da altro atto giuridico**, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, prevede nel dettaglio **le regole e i limiti** con cui devono essere trattati i dati personali.

Addendum contrattuale tra titolare e responsabile deve definire:

- La materia disciplinata
- La durata del trattamento
- La natura e finalità del trattamento
- Il tipo di dati personali
- Le categorie di interessati
- Gli obblighi e diritti del responsabile del trattamento

Il contratto tra titolare e responsabile deve inoltre prevedere che il responsabile:

- **tratti i dati personali soltanto su istruzione documentata del titolare del trattamento (…).** Le Linee Guida EDPB raccomandano espressamente di includere al Contratto un allegato che dia conto in modo specifico tramite procedure o template delle istruzioni che il responsabile è tenuto a rispettare

- garantisca che **le persone autorizzate** al trattamento dei dati personali si siano **impegnate alla riservatezza** o abbiano un adeguato obbligo statutario di riservatezza;

- **adotti tutte le misure (di sicurezza) richieste ai sensi dell'articolo 32:** il contratto non può limitarsi a ribadire pedissequamente il dettato normativo, ma deve includere una descrizione precisa e completa delle misure che si intendono adottare. Il livello di dettaglio delle misure di sicurezza dipenderà inoltre dall'analisi del caso concreto alla luce, basata sulla preventiva analisi dei rischi. Per facilitare il lavoro ed alleggerire il documento finale, le Linee Guida EDPB consigliano di predisporre le misure di sicurezza come allegato al Contratto.

Il contratto tra titolare e responsabile deve inoltre prevedere che il responsabile:

- **rispetti le condizioni per ricorrere a un altro responsabile del trattamento (sub-responsabile):** Il contratto deve specificare il divieto per il responsabile di fare ricorso a un altro responsabile senza una previa autorizzazione scritta da parte del titolare, che può essere specifica o generale.

In caso di autorizzazione specifica, deve essere individuato il sub-responsabile nonché le specifiche attività di trattamento oggetto del Contratto. Il silenzio da parte del titolare verso una richiesta di autorizzazione del responsabile sarà da intendersi quale rifiuto (silenzio-diniego).
L'autorizzazione generale, al contrario, impone al responsabile di informare in anticipo il titolare di eventuali modifiche relative all'aggiunta o sostituzione di altri sub responsabili, dando in tal modo la possibilità al titolare di opporsi a tali modifiche (silenzio-assenso), alla luce di criteri valutabili (es. risorse, affidabilità, esperienza, ecc.).

(***segue)***

- **assista il titolare** del trattamento con misure tecniche ed organizzative adeguate al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per **l'esercizio dei diritti dell'interessato**;

- **assista il titolare** del trattamento nel garantire il **rispetto degli obblighi di cui agli articoli da 32 a 36 (sicurezza; data breaches; DPIA**), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

- su scelta del titolare del trattamento, **cancelli o gli restituisca** tutti i dati personali dopo che è terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti;

- **metta a disposizione** del titolare del trattamento tutte **le informazioni** necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca agli audit, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Il rischio risarcitorio: art. 82 Reg. UE 2016/679:

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento**.**

2. 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.

3. 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.

4. **Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento** e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, **ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.**

Il rischio risarcitorio: art. 82 Reg. UE 2016/679:

Considerando numero 85

fornisce un elenco esemplificativo delle tipologie dei danni patiti dalle persone fisiche, che potrebbero conseguire a una violazione di dati personali. Tale elenco è raggruppabile in tre tipologie quali:

1) i danni fisici
2) i danni materiali
3) ed i danni immateriali.

Si pensi, ad esempio: alla perdita del controllo sui dati da parte dell'interessato, al furto d'identità, al pregiudizio della reputazione.