LE NUOVE NORME SULLA PRIVACY:

OBBLIGHI E ADEMPIMENTI DELLE IMPRESE

Padova, 11 aprile 2018

DOVERI E RESPONSABILITÀ DEL TITOLARE SANZIONI

AVV. GIOVANNI TAGLIAVINI

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 dati personali.

Titolare del trattamento – Doveri e compiti

Il titolare del trattamento mette in atto le misure tecniche e organizzative adeguate a garantire e dimostrare la conformità dei trattamenti al GDPR.

A tal fine, egli:

- esegue, ove necessario, la valutazione d'impatto sulla protezione dei dati (DPIA – art. 35 GDPR);
- implementa le misure di sicurezza, quali pseudonimizzazione e cifrature dati (art. 32 GDPR);
- cura, ove necessario, la tenuta del Registro dei trattamenti (art. 30 GDPR);
- provvede alla notifica delle violazioni riscontrate (artt. 33-34 GDPR).

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.

Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a garantire la conformità del trattamento al GDPR.

La nomina avviene attraverso un contratto scritto, che indica:

- la materia disciplinata e la durata del trattamento;
- la natura e la finalità del trattamento;
- il tipo di dati personali trattati e le categorie di interessati;
- gli obblighi e i diritti del titolare del trattamento.

Il responsabile del trattamento deve:

- trattare i dati nel rispetto delle istruzioni del titolare;
- garantire l'impegno alla riservatezza delle persone da lui autorizzate al trattamento (ad es., collaboratori);
- assistere il titolare al fine di soddisfare l'esercizio dei diritti degli interessati;
- cancellare o restituire i dati trattati quando termina la prestazione dei servizi;
- mettere a disposizione del titolare gli elementi per dimostrare la conformità al GDPR.

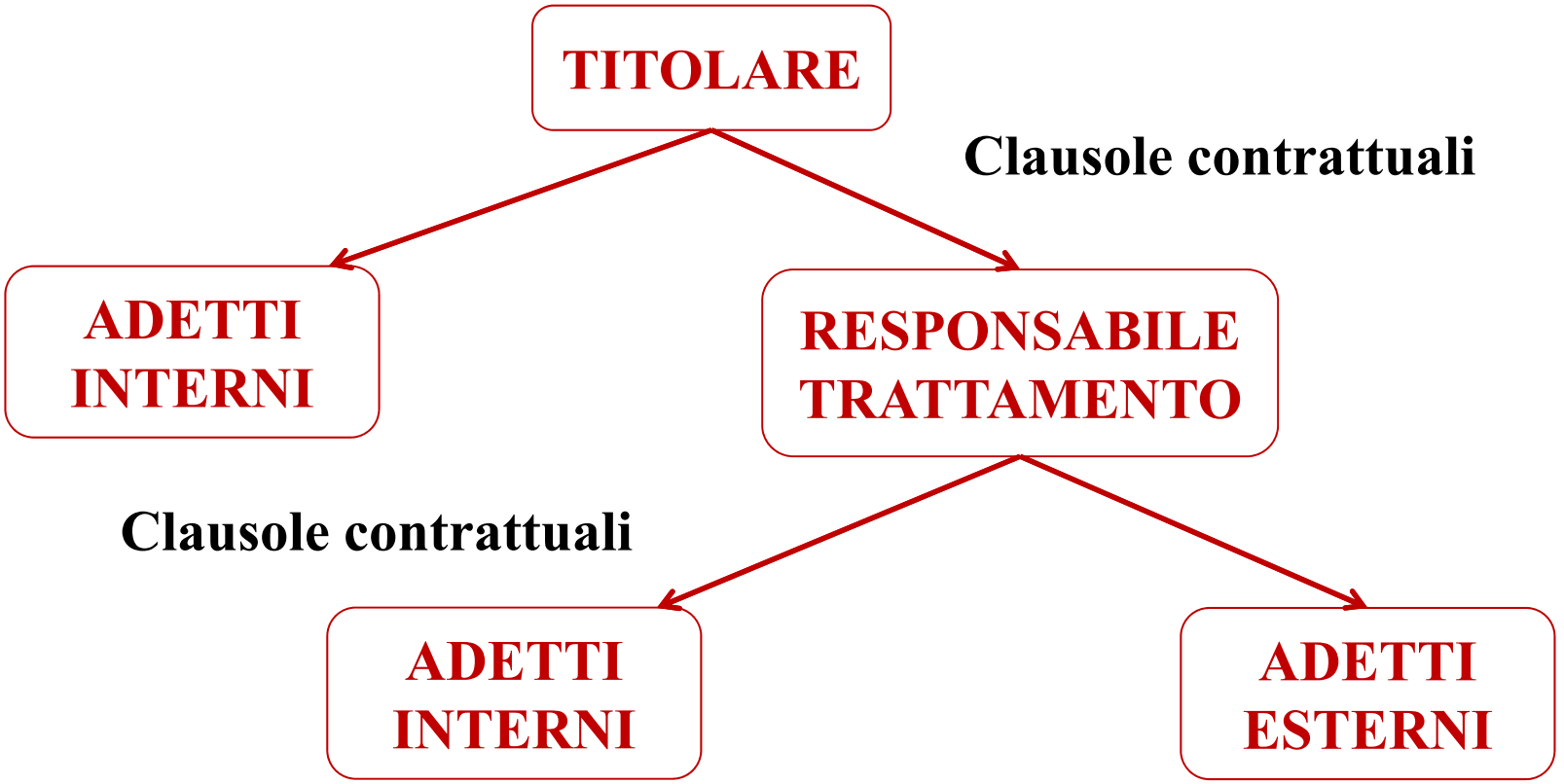
Il responsabile del trattamento non può ricorrere a sua volta ad un altro responsabile, salvo autorizzazione espressa del titolare. Eventuali inadempimenti del sub responsabile gravano interamente a carico del responsabile iniziale.

Qualora il responsabile del trattamento viola il GDPR, determinando le finalità e i mezzi del trattamento, è considerato titolare del trattamento in questione.

I soggetti «incaricati»

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.

Il titolare, prima di avvalersi di altri soggetti, deve provvedere alla loro autorizzazione mediante nomina espressa per iscritto.


TITOLARE
Clausole contrattuali
ADETTI INTERNI
RESPONSABILE TRATTAMENTO
Clausole contrattuali
ADETTI INTERNI
ADETTI ESTERNI

Responsabile della protezione dati (DPO)

È la persona fisica che si occupa di informare e fornire assistenza al titolare (o al responsabile) ed ai suoi dipendenti che eseguono il trattamento dei dati.

Egli valuta altresì il grado di conformità dell'organizzazione alla normativa in punto di protezione dei dati, presta assistenza nella redazione della DPIA e funge da punto di contatto per il Garante.

A tal fine, deve essere in possesso di elevate qualità professionali e di conoscenza specialistica della normativa.

Il DPO può essere un soggetto esterno o interno (dipendente), ma devono essergli garantite autonomia organizzativa ed adeguate risorse, anche finanziarie.

Non può rivestire tale ruolo chi all'interno dell'organizzazione del titolare o del responsabile abbia un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali.

Un gruppo può nominare un unico DPO, a condizione che sia facilmente raggiungibile da ciascuno stabilimento.

Nomina obbligatoria quando:

- Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

- Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in:

  - trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
  - trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.

RESPONSABILITÀ E SANZIONI

Violazione di dati personali

Qualsiasi 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 trasmetti, conservati o comunque trattati.

Possibili conseguenze della violazione

- Azioni legali e costi di difesa derivanti da richiesta di risarcimento o per violazione di obblighi di riservatezza;
- Pregiudizi in termini di *brand reputation*;
- Sanzioni amministrative a carico dell'ente;
- Sanzioni penali

Danno cagionato per effetto del trattamento

Ai sensi dell'art. 15 del Codice della Privacy, il trattamento illecito di dati personali determina l'insorgere di una responsabilità risarcitoria ex art. 2050 c.c. in ragione dello svolgimento di attività c.d. pericolosa.

Il risarcimento è dovuto **anche in caso di violazione dell'art. 11 (Modalità del trattamento e requisiti dei dati).**

Il Reg. UE 2016/679 conferma il diritto al risarcimento

Ai sensi dell'art. 82 GDPR, chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Il titolare o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Responsabilità solidale

Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni titolare e responsabile del trattamento risponde in solido per l'intero ammontare del danno, salvo diritto di regresso interno.

Sanzioni amministrative pecuniarie

- fino a 10.000.000 di Euro per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione di determinati obblighi imposti dal Regolamento (es. Registro Trattamenti, DPO)
- fino a 20.000.000 di euro per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione degli obblighi ritenuti più rilevanti (es. violazione principi generali ex artt. 5, 6, 7 e 9)

Sanzioni penali

Non è materia di competenza dell'UE. È compito degli Stati membri stabilire (e notificare alla Commissione entro il 25 maggio 2018) le norme relative alle altre sanzioni per le violazioni del Regolamento e adottare tutti i provvedimenti necessari per assicurare l'applicazione di sanzioni effettive, proporzionate e dissuasive.

Il decreto di coordinamento prevede l'abrogazione dell'art. 167 del Codice della Privacy (Trattamento illecito di dati)

CORTELLAZZO & SOATTO
Economia Diritto e Finanza di Impresa

Via Porciglia, 14 – Padova
Via Tuveri, 25 – Cagliari
www.cortellazzo-soatto.it