G.D.P.R. Parte Seconda

Regolamento generale sulla protezione dei dati personali

G.D.P.R.

Gli adempimenti documentali

FAQ sul registro delle attività di trattamento – Garante Privacy

Registro dei trattamenti

L'art. 30 del Regolamento (UE) n. 679/2016 (di seguito "RGPD") prevede tra gli adempimenti principali del titolare e del responsabile del trattamento la tenuta del **registro delle attività di trattamento**.

È un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Registro dei trattamenti

Il Registro dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati dal titolare o responsabile.

In quanto tale, il registro deve essere **mantenuto costantemente aggiornato** poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere.

Qualsiasi cambiamento, in particolare in ordine alle **modalità, finalità, categorie di dati, categorie di interessati,** deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, **la data della sua prima istituzione** (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) **unitamente a quella dell'ultimo aggiornamento**. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

"- scheda creata in data XY"

"- ultimo aggiornamento avvenuto in data XY"

FAQ sul registro delle attività di trattamento – Garante Privacy

Registro dei trattamenti

CHI DEVE REDIGERE IL REGISTRO?

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il Registro delle attività di trattamento (v. art. 30, par. 1 e 2 del RGPD).

In particolare, in ambito privato, i soggetti obbligati sono così individuabili:

a) **imprese o organizzazioni con almeno 250 dipendenti**;

b) **qualunque titolare o responsabile** (incluse imprese o organizzazioni con meno di 250 dipendenti) **che effettui trattamenti che possano presentare un rischio** – anche non elevato – per i diritti e le libertà dell'interessato;

c) **qualunque titolare o responsabile** (incluse imprese o organizzazioni con meno di 250 dipendenti) **che effettui trattamenti non occasionali**;

d) **qualunque titolare o responsabile** (incluse imprese o organizzazioni con meno di 250 dipendenti) **che effettui trattamenti delle categorie particolari** di dati di cui all'articolo 9, paragrafo 1 RGPD, **o di dati personali relativi a condanne penali** e a reati di cui all'articolo 10 RGPD.

Rientrano nella categoria delle "organizzazioni" di cui all'art. 30, par. 5 anche le associazioni, fondazioni e i comitati.

FAQ sul registro delle attività di trattamento – Garante Privacy

Registro dei trattamenti

CHI DEVE REDIGERE IL REGISTRO?

Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del registro, ad esempio:

a) **esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente** (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);

b) **liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati** (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);

c) **associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati** (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);

d) **il condominio ove tratti "categorie particolari di dati"** (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Guida del Garante Privacy

Raccomandazione

Registro dei trattamenti

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali.**

Per tale motivo si invitano tutti i titolari e responsabili del trattamento, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Registro dei trattamenti

QUALI INFORMAZIONI DEVE CONTENERE IL REGISTRO?

a) “dati di contatto del titolare del trattamento e del D.P.O. (se presente)”;

b) “finalità del trattamento”: oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso.

Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di “categorie particolari di dati”, indicare una delle condizioni di cui all’art. 9, par. 2 del RGPD; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell’Unione europea) che ne autorizza il trattamento ai sensi dell’art. 10 del RGPD.

Art. 30
REG. EU 679/2016

Registro dei trattamenti

QUALI INFORMAZIONI DEVE CONTENERE IL REGISTRO?

c) **“descrizione delle categorie di interessati e delle categorie di dati personali”** andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.).

d) **“categorie di destinatari a cui i dati sono stati o saranno comunicati”** andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi).

Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub-responsabili del trattamento– siano trasmessi i dati da parte del titolare (es. soggetto esterno cui sia affidato dal titolare il servizio di elaborazione delle buste paga dei dipendenti o altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento).

Ciò al fine di consentire al titolare medesimo di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali.

Art. 30
REG. EU 679/2016

Registro dei trattamenti

QUALI INFORMAZIONI DEVE CONTENERE IL REGISTRO?

e) "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" andrà riportata l'informazione relativa ai suddetti trasferimenti unitamente all'indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle "garanzie" adottate ai sensi del capo V del RGPD (es. decisioni di adeguatezza, norme vincolanti d'impresa, clausole contrattuali tipo, ecc.).

f) "termini ultimi previsti per la cancellazione delle diverse categorie di dati" dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento (ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione – v. art. 2220 del codice civile"). Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri (es. norme di legge, prassi settoriali) indicativi degli stessi (es. "in caso di contenzioso, i dati saranno cancellati al termine dello stesso").

Art. 30
REG. EU 679/2016

Registro dei trattamenti

QUALI INFORMAZIONI DEVE CONTENERE IL REGISTRO?

g) "descrizione generale delle misure di sicurezza" andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'art. 32 del RGDP tenendo presente che l'elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimessa al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere.

Tale lista ha di per sé un carattere dinamico (e non più statico come è stato per l'Allegato B del d. lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l'insorgere di nuovi rischi.

Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale (es. procedure organizzative interne; security policy ecc.).

Può essere riportata nel registro qualsiasi altra informazione che il titolare o il responsabile ritengano utile indicare (ad es. le modalità di raccolta del consenso, le eventuali valutazioni di impatto effettuate, l'indicazione di eventuali "referenti interni" individuati dal titolare in merito ad alcune tipologie di trattamento ecc.).

Art. 30
REG. EU 679/2016

Registro dei trattamenti

IL REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento tiene un registro di **"tutte le categorie di attività relative al trattamento svolte per conto di un titolare"** (art. 30, par. 2 del RGPD).

In merito alle modalità di compilazione dello stesso si rappresenta quanto segue:

a) nel caso in cui uno stesso soggetto agisca in qualità di **responsabile del trattamento per conto di più clienti** quali autonomi e distinti titolari (es. società di software house), le informazioni di cui all'art. 30, par. 2 del RGPD dovranno essere riportate nel registro **con riferimento a ciascuno dei suddetti titolari.**

In questi casi il responsabile dovrà **suddividere il registro in tante sezioni** quanti sono i titolari per conto dei quali agisce; ove, a causa dell'ingente numero di titolari per cui si operi, l'attività di puntuale indicazione e di continuo aggiornamento dei nominativi degli stessi nonché di correlazione delle categorie di trattamenti svolti per ognuno di essi risulti eccessivamente difficoltosa**, il registro del responsabile potrebbe riportare il rinvio, ad es., a schede o banche dati anagrafiche dei clienti (titolari del trattamento), contenenti la descrizione dei servizi forniti agli stessi**, ferma restando la necessità che comunque tali schede riportino tutte le indicazioni richieste dall'art. 30, par. 2 del RGPD.

Art. 30
REG. EU 679/2016

Registro dei trattamenti

IL REGISTRO DEL RESPONSABILE DEL TRATTAMENTO

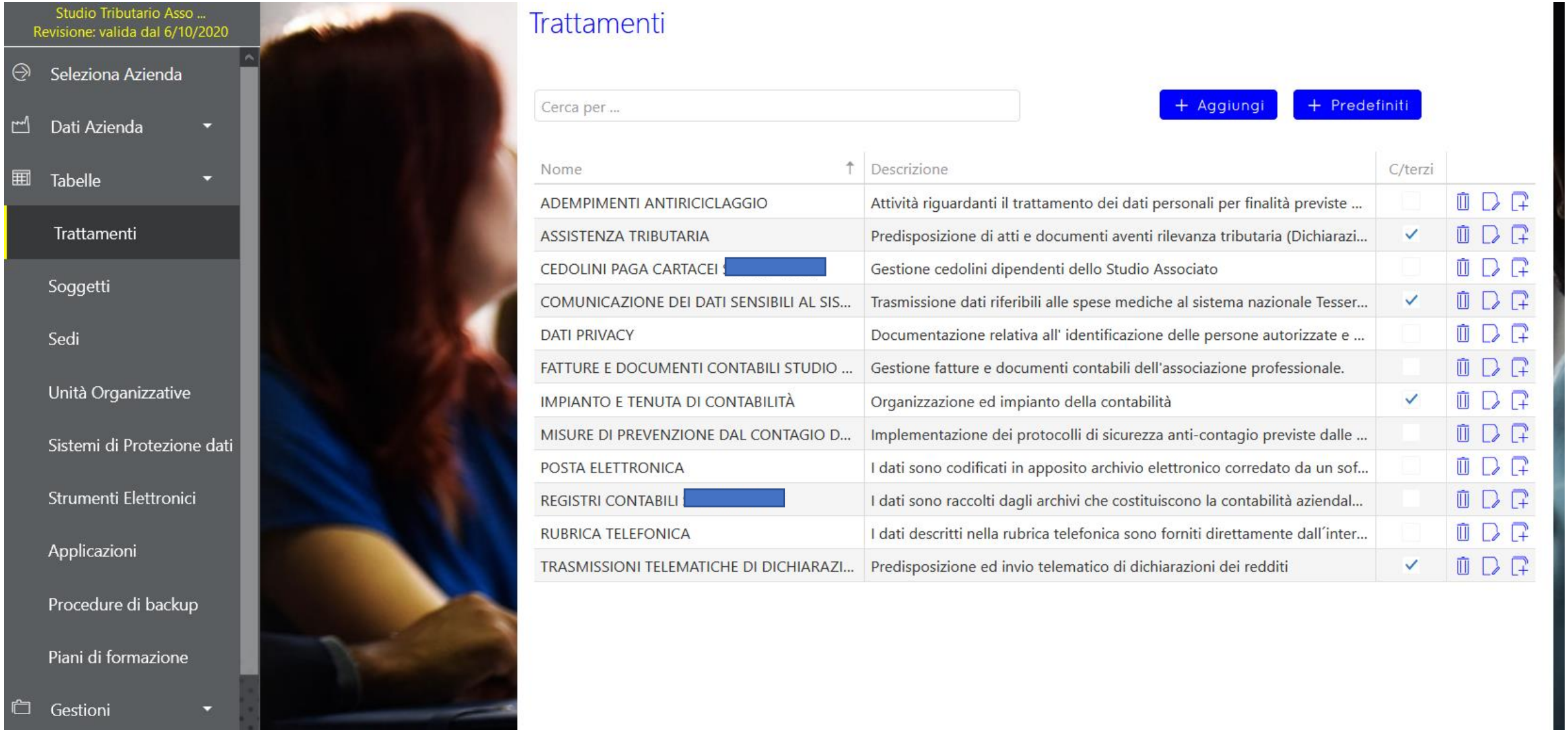
b) con riferimento alla **"descrizione delle categorie di trattamenti effettuati"** (art. 30, par. 2, lett. b) del RGPD) è possibile far riferimento a quanto contenuto nel contratto di designazione a responsabile che, ai sensi dell'art. 28 del RGPD, deve individuare, in particolare, **la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati oggetto del trattamento, nonché la durata di quest'ultimo**;

c) **in caso di sub-responsabile**, parimenti, **il registro delle attività di trattamento svolte da quest'ultimo** potrà specificatamente far riferimento ai contenuti del contratto stipulato tra lo stesso e il responsabile ai sensi dell'art. 28, paragrafi 2 e 4 del RGPD.

Art. 30
REG. EU 679/2016

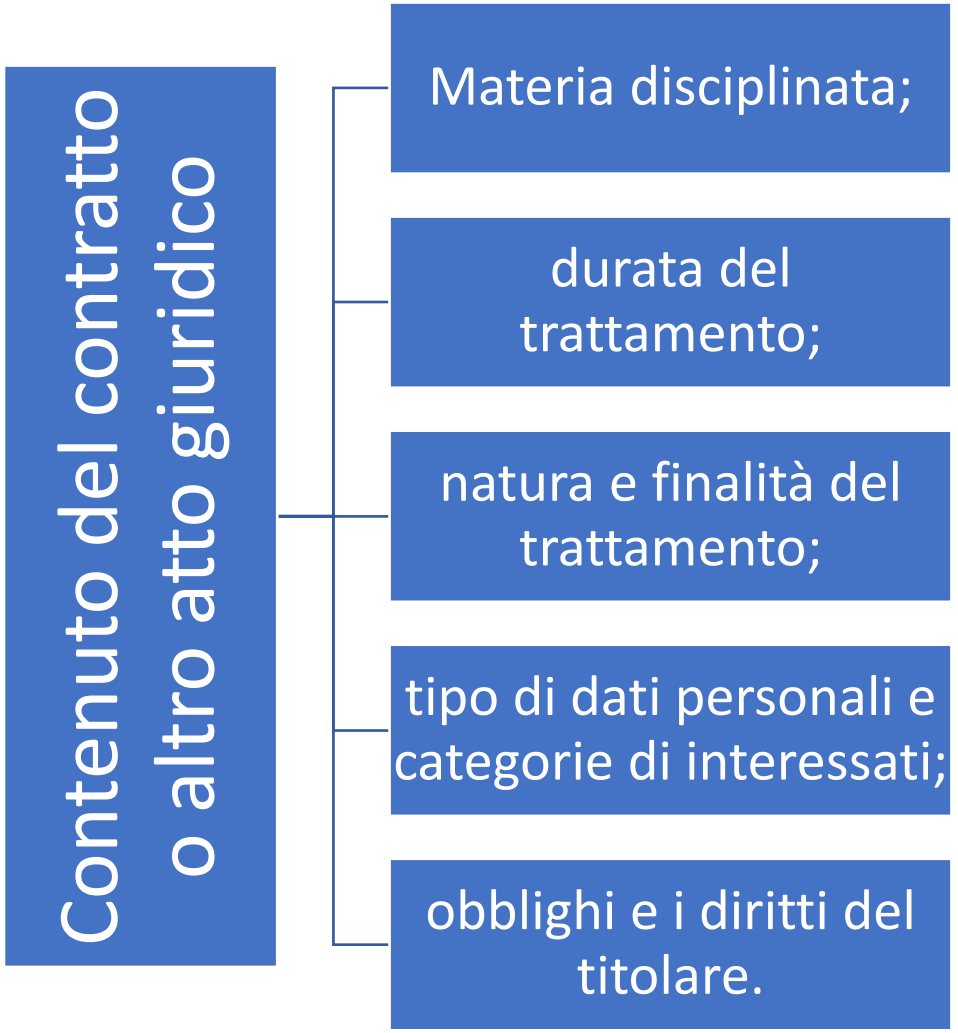
Il Registro dei trattamenti

Registro dei trattamenti



Nomina del responsabile del trattamento (art. 28)

PREMESSA
Qualora un trattamento debba essere 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**.



Obblighi del responsabile del trattamento (art. 28.3)

a) trattare i dati solo su istruzioni documentate del titolare;

b) assicurare che gli incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adottare tutte le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32;

d) ricorrere ad un altro responsabile (SUBRESPONSABILE) solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento;

e) assistere il titolare con adeguate misure, tecniche ed organizzative, per «dar seguito alle richieste per l'esercizio dei diritti dell'interessato»;

Obblighi del responsabile del trattamento (art. 28.3)

f) assistere il titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (misure tecniche, data breach, dpia), tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile;

g) cancellare tutti i dati personali o restituire le copie esistenti alla cessazione delle funzioni di Responsabile;

h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e collaborazione alle attività di revisione, comprese le ispezioni realizzate dal Titolare o da un altro soggetto da questi incaricato. 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.

Nomina del Sub-responsabile del trattamento (art. 28.2 e 28.4)

Il 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.

Quando 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.

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.

Analisi dei rischi

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Analisi dei rischi

Il primo fra tali criteri è sintetizzato dall'espressione inglese **«data protection by default and by design»**, ossia dalla necessità di configurare il trattamento prevedendo **fin dall'inizio** le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei **rischi** per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, **prima di procedere al trattamento dei dati vero e proprio** ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Analisi dei rischi

Il secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari è quello del rischio inerente i trattamenti.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare. All'esito di questa valutazione di impatto il titolare deciderà in autonomia se iniziare il trattamento o consultare l'autorità di controllo per ottenere informazioni su come gestire il rischio residuale. L'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Approccio basato sul rischio

La valutazione dei rischi deve tener conto di : **distruzione, perdita, modifica, rivelazione o accesso non autorizzato a dati personali trasmessi , conservati o elaborati.**