

PRIVACY

Registro dei trattamenti
Note informative

Ottobre 2018

Documento interno
a cura dell'Ufficio privacy

Cosa è il registro delle attività di trattamento?

L'articolo 30 del Regolamento (EU) n. 679/2016 prevede, tra gli adempimenti principali del titolare e del responsabile del trattamento, la tenuta del registro delle attività di trattamento.

Si tratta di un documento contenente le principali informazioni (specificamente individuate dall'articolo 30) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento.

Il registro costituisce anche 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.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante per la protezione dei dati personali.

Chi è tenuto a redigerlo?

Tutti i titolari e i responsabili del trattamento sono tenuti a redigere il registro delle attività di trattamento. Al di fuori dei casi di tenuta obbligatoria del registro, il Garante per la protezione dei dati personali ne raccomanda, in ogni caso, la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di *accountability* e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso.

Quali informazioni deve contenere?

Il Regolamento individua le informazioni che devono essere contenute nel registro delle attività di trattamento del titolare (articolo 30, par. 1) e in quello del responsabile (articolo 30, par. 2).

Con riferimento ai contenuti si precisa quanto segue:

- a) nel campo "finalità del trattamento", oltre all'indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro), occorre indicare anche la base giuridica (articolo 6);
- b) nel campo "descrizione delle categorie di interessati e delle categorie di dati personali", devono essere specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, dati relativi a condanne penali o reati, ecc.);
- c) nel campo "categorie di destinatari a cui i dati sono stati o saranno comunicati", devono essere riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui i dati siano comunicati. Inoltre, devono essere indicati anche gli eventuali altri soggetti ai quali, in qualità di responsabili del trattamento, i dati siano trasmessi per le finalità perseguite con il trattamento;
- d) nel campo "termini ultimi previsti per la cancellazione delle diverse categorie di dati", devono essere individuati i tempi di cancellazione per tipologia e finalità di trattamento. 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 in materia di archiviazione dei documenti pubblici) sull'indicazione degli stessi;
- e) nel campo "descrizione generale delle misure di sicurezza", andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell'articolo 32, 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 fornire 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.).

Nel registro può essere riportata 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.).

Quali sono le modalità di conservazione e di aggiornamento?

Il Registro dei trattamenti è un documento di censimento e di 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 deve 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 un'annotazione del tipo:

“- scheda creata in data ...”

“- ultimo aggiornamento avvenuto in data ...”

Modalità operative per il registro delle attività di trattamento della Regione.

La Regione si è dotata di un applicativo (DPM – Data Protection Manager) che consentirà di elaborare un registro in forma elettronica. L'applicativo è stato popolato con i trattamenti e le informazioni contenuti nel Documento Programmatico per la Sicurezza (DPS).

L'applicativo sarà accessibile all'interno della Intranet regionale con le credenziali di rete. Tutti i dipendenti potranno accedere e visionare i trattamenti per cui sono stati autorizzati, la propria lettera di incarico e gli eventuali corsi di formazione che si prevede di erogare in modalità *e-learning*. I dirigenti/delegati potranno accedere e modificare tutti i trattamenti di competenza della struttura; per la compilazione del registro, potranno autorizzare uno o più dipendenti per ciò che attiene ai trattamenti di competenza.