DOC. N. 6

Registro dei trattamenti privacy: istruzioni e soggetti obbligati

Secondo le istruzioni pubblicate sul sito dell'Autorità Garante della Privacy e redatte sulla base delle novità introdotte dal GDPR, il registro dei trattamenti dovrà essere compilato in forma scritta, in modalità cartacea ed elettronica.

L'obbligo di redigere il Registro - RGDP - riguarda i seguenti soggetti privati:

- le imprese o le organizzazioni con almeno 250 dipendenti;
- 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;
- qualunque titolare o responsabile (incluse imprese o organizzazioni con meno di 250 dipendenti) che effettui trattamenti non occasionali;
- 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.

È quindi chiaro che sono obbligati a tenere e redigere il registro dei trattamenti dei dati personali buona parte di imprese e professionisti.
Ad esempio, il RGPD è obbligatorio per negozi, uffici o artigiani (bar, ristoranti) con almeno un dipendente, così come per chi tratta dati sanitari dei propri clienti (come parrucchieri, estetisti, ottici, tatuatori ecc..). L'obbligo riguarda anche i liberi professionisti, come commercialisti, notai, avvocati, farmacisti o medici in generale, che trattano dati sanitari o "sensibili".
Nelle istruzioni pubblicate dall'Autorità Garante è specificato inoltre che anche le associazioni, le fondazioni o i comitati sono obbligati a redigere il registro dei trattamenti ai fini del rispetto del GDPR qualora trattino categorie particolari di dati. Si tratta ad esempio di associazioni che si occupano di soggetti vulnerabili (disabili, ex detenuti, ecc..) o associazioni che perseguono finalità di contrasto alle discriminazioni di genere, razziale, basate sull'orientamento religioso, sessuale o politico, così come le associazioni sportive che trattano dati sanitari o i partiti e sindacati.

Per le imprese e le organizzazioni con meno di 250 dipendenti sono previste misure di semplificazione e il Garante Privacy ha pubblicato un modello di registro dei trattamenti appositamente dedicato.

Registro dei trattamenti privacy, modello semplificato per le PMI

Così come chiarito nelle istruzioni pubblicate dal Garante, le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno beneficiare di alcune misure di semplificazione.

In tal caso l'obbligo di redazione del registro riguarderà soltanto le specifiche attività di trattamento sopra individuate (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento).

Per semplificare il rispetto degli adempimenti previsti dal GDPR alle PMI, il Garante Privacy ha pubblicato l'8 ottobre 2018 due modelli relativi al registro semplificato per il responsabile del trattamento e per il titolare.

Di seguito si forniscono le ulteriori istruzioni per la compilazione e la tenuta del Registro secondo quanto riportato nella pagina dedicata sul sito del Garante Privacy.

Registro dei trattamenti: istruzioni compilazione del Garante Privacy

Le istruzioni su come compilare il registro dei trattamenti sono contenute nel GDPR e a riassumere è l'Autorità Garante per la privacy.

In merito ai contenuti, bisognerà compilare i seguenti dati:

- nel campo **"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 (v. art. 6 del RGPD; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare (v. provv. del Garante del 22 febbraio 2018 – [doc web n. 8080493]). 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. 2del 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;

- nel campo **"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.);
- nel campo **"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;
- nel campo **"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.);
- nel campo **"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");
- nel campo **"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.).

Modalità di conservazione e di aggiornamento del Registro dei trattamenti

Il Registro dei trattamenti dovrà essere costantemente aggiornato in quanto si tratta di un documento indispensabile per dimostrare le attività di trattamento dati effettuate dal titolare o dal responsabile.

In merito alle modalità di tenuta e conservazione, il Garante ricorda che potrà essere compilato sia in formato cartaceo che elettronico e che dovrà indicare 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.

Nel caso di aggiornamento, nel Registro bisognerà indicare un'annotazione del seguente tipo:

- "scheda creata in data XY", ultimo aggiornamento avvenuto in data XY"

Registro responsabile trattamento dati

In chiusura, nelle istruzioni fornite dal Garante per la Privacy è chiarito che il responsabile del trattamento deve tenere un registro di "tutte le categorie di attività relative al trattamento svolte per conto di un titolare".

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

- 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;

- 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;
- 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.