collana legale

GDPR:
Aggiornamento alla luce delle istruzioni fornite dall'Autorità Garante per la protezione dei dati personali in data 08 ottobre 2018

parte 2

GDPR:
Aggiornamento alla luce delle istruzioni fornite dall'Autorità Garante per la protezione dei dati personali in data 08 ottobre 2018

a cura
di Maurizio Flick

FLA
FEDERLEGNOARREDO

S O M M A R I O

Premessa

L'Autorità Garante per la protezione dei dati personali l'8 ottobre 2018 ha pubblicato un documento esplicativo sul Registro delle attività di trattamento. L'intervento dell'Autorità vuole chiaramente fornire soluzioni pratiche e spiegazioni sul contenuto del Registro e sui soggetti tenuti alla redazione dello stesso nonché modelli di "Registro semplificato" delle attività di trattamento sia del titolare che del responsabile per le Piccole e Medie Imprese.

Il Garante, in particolare, con tale provvedimento intende aiutare le PMI nella ***compliance*** **al GDPR** fornendo due **schemi pronti** alla compilazione, rispettivamente per le figure di titolare e responsabile.

Il documento pubblicato dal Garante ricomprende vere e proprie FAQ, ossia le risposte alle domande più frequenti rivolte all'Ufficio del Garante circa obblighi e modalità di tenuta del Registro stesso.

Dunque, un **modello** semplificato per le **PMI** e regole meno stringenti per imprese e attività con un solo dipendente con riferimento all'adempimento previsto *dall'articolo 30* del Regolamento europeo, in base al quale il titolare del trattamento e il suo rappresentante sono obbligati a tenere un Registro delle **attività di trattamento** svolte sotto la propria responsabilità, in cui bisogna indicare una serie precisa di informazioni (finalità del trattamento, categorie di dati personali, persone a cui vengono comunicati, regola per la cancellazione, misure di sicurezza, etc…).

L'obbligo di redigere questo Registro, specifica il Garante, rappresenta: *"uno dei principali elementi di* **accountability**[1] *del titolare, poiché rappresenta uno strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile ai fini della valutazione o analisi del rischio e dunque preliminare rispetto a tale attività".*

Il Registro delle attività di trattamento privacy deve essere tenuto in forma scritta, eventualmente anche elettronica, e deve essere esibito su richiesta al Garante.

In base al GDPR, l'**obbligo** riguarda tutte le imprese sopra i 250 dipendenti e le PMI sotto tale soglia nel caso in cui trattino **dati sensibili**, ossia:

- trattamenti che possano presentare un **rischio** – anche non elevato – per i diritti e le libertà dell'interessato;
- trattamenti di dati **non occasionali**;
- **dati sensibili** elencati nell'articolo 9 del GDPR (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale). Dati relativi a condanne penali o reati (articolo 10 GDPR).

Quindi, chiarisce ulteriormente il Garante nelle **FAQ**, sono tenuti a predisporre il Registro le seguenti **categorie di piccole imprese**:

[1] Il principio di accountability, ossia il principio di responsabilizzazione (previsto dall'ultimo comma dell'art. 5 GDPR) in base al quale, tra l'altro, occorre essere in grado di comprovare (a posteriori evidentemente) di aver rispettato puntualmente i principi applicabili al trattamento dei dati personali. Il Registro delle attività di trattamento, pertanto, è uno strumento utile - sia al titolare che al responsabile – per dimostrare come, in ogni tempo e in ogni fase del trattamento, si siano applicati i principi del GDPR e come si sia adempiuto agli obblighi derivanti dal trattamento dei dati personali.

- **esercizi commerciali,** esercizi pubblici o **artigiani con almeno un dipendente** (bar, ristoranti, officine, **negozi, piccola distribuzione**);
- **esercizi commerciali**, esercizi pubblici o artigiani che trattano dati sanitari dei clienti (parrucchieri, estetisti, ottici, odontotecnici, tatuatori);
- liberi professionisti con almeno un dipendente;
- liberi professionisti che trattano dati sanitari oppure relativi a condanne penali o reati (commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);
- associazioni, fondazioni e comitati che trattano categorie particolari di dati e/o dati relativi a condanne penali o reati (organizzazioni di tendenza, associazioni a tutela di soggetti vulnerabili quali ad esempio malati, persone con disabilità, ex detenuti, associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso, associazioni sportive con riferimento ai dati sanitari trattati, partiti e movimenti politici, sindacati, associazioni e movimenti a carattere religioso);
- il condominio ove tratti "categorie particolari di dati", come 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).

Le PMI possono compilare questo Registro in forma semplificata, limitandosi a indicare le attività sopra specificate. Ad esempio, un'impresa con un solo dipendente può predisporre il Registro Privacy esclusivamente con riferimento a tale limitata tipologia di trattamento. Sul sito del Garante sono pubblicati i **modelli semplificati** per il titolare e per il responsabile del trattamento delle PMI che si riportano *infra*.

Il Registro Privacy deve essere costantemente aggiornato. 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) e quella dell'ultimo aggiornamento.

Il Garante consiglia di tenere il Registro Privacy anche ai soggetti non obbligati, perché contribuisce ad attuare, con modalità semplici e accessibili a tutti, il principio di *account*ability e, al contempo, agevolando l'attività del Garante.

Di seguito si riportano le 6 FAQ predisposte dall'Autorità Garante con un breve commento di ausilio per le imprese.

1. Cos'è il Registro delle attività di trattamento?

La prima FAQ predisposta dall'Autorità Garante è tesa a individuare, innanzitutto, in cosa consista il Registro previsto dall'art. 30 del GDPR o, meglio, i **registri delle attività di trattamento**. I primi due commi dell'art. 30 del GDPR, infatti, prevedono due distinti registri: il Registro del titolare del trattamento e il Registro del responsabile del trattamento (di cui all'art. 28 del GDPR).

Elemento comune ai registri - e da questo punto di vista le FAQ del Garante italiano ribadiscono, esplicitandolo, il contenuto dell'art. 30 del GDPR - è che si tratti di un

documento che ha **forma scritta** (anche in "**formato elettronico**", come prevede il terzo comma del medesimo art. 30 GDPR) e che deve essere istituito e tenuto aggiornato sia dal titolare del trattamento che da parte del **responsabile del trattamento**. Qualora un singolo soggetto (sia esso persona fisica, ente o organismo pubblico) assommi in sé, in relazione a diverse ipotesi di trattamento, la veste di titolare del trattamento e quella di responsabile del trattamento, allora dovrà tenere entrambi i registri: sia quello prescritto in capo al titolare del trattamento (primo comma dell'art. 30) che quello del responsabile del trattamento (secondo comma dell'art. 30).

Attraverso lo strumento del Registro del trattamento, evidenzia il Garante, si esprime quello che può essere considerato, a ragione, uno dei principali e fondanti principi dell'impianto del GDPR: il **principio di *accountability*** ossia il principio di responsabilizzazione (previsto dall'ultimo comma dell'art. 5 del GDPR) in base al quale, tra l'altro, occorre essere in grado di comprovare (a posteriori, evidentemente) di aver rispettato puntualmente i principi applicabili al trattamento dei dati personali. Il Registro delle attività di trattamento, pertanto, è uno strumento utile - sia al titolare che al responsabile - per dimostrare come, in ogni tempo e in ogni fase del trattamento, si siano applicati i principi del GDPR e come si sia adempiuto agli obblighi derivanti dal trattamento dei dati personali.

Nelle FAQ il Garante evidenzia, oltretutto, la duplice funzione del Registro dei trattamenti: da un lato consente a titolare e responsabile del trattamento di delineare il quadro (da tenere costantemente aggiornato) del quadro dei trattamenti in essere all'interno della propria organizzazione al fine di consentirgli di eseguire una puntuale valutazione e analisi dei rischi incombenti sui dati personali sottoposti a trattamento e, dall'altro, consente a titolare e responsabile di dimostrare - anche in conseguenza di un'eventuale attività ispettiva da parte del Garante che può richiedere l'esibizione dei registri del trattamento - il summenzionato quadro dei trattamenti e la sua evoluzione nel corso del tempo.

Ed è proprio per questo motivo, ad esempio, che nella FAQ n. 5 si prevede la necessità di tenere costantemente aggiornato il Registro (sia quello del titolare che quello del responsabile del trattamento) e di tenere traccia delle modifiche (relative a modalità, finalità, categorie di dati, categorie di interessati del trattamento) che nel corso del tempo dovessero apportarsi al Registro dei trattamenti.

A questo proposito si prevede che il Registro debba recare "in maniera verificabile" sia la data della sua prima istituzione o creazione sia la data dell'ultimo aggiornamento. Il concetto di "maniera verificabile" sembrerebbe richiamare quello di data certa anche se non espressamente previsto dalla FAQ in questione. La FAQ in questione non prevede - anche se sarebbe particolarmente utile nell'ottica dell'*accountability* sia a titolari che a responsabili del trattamento - la necessità di tenere traccia oltre che della data di creazione e di ultima modifica anche di ogni data di modifica sostanziale (ossia, come visto, di ogni modifica relativa a modalità, finalità, categorie di dati, categorie di interessati del trattamento). In tal modo, infatti, potrebbe ricostruirsi il contenuto del Registro "vigente" ad una determinata data.

Di seguito il testo della FAQ n. 1 *Cos'è il registro delle attività di trattamento?* predisposta dall'Autorità Garante per la protezione dei dati personali pubblicata l'8 Ottobre 2018 sul sito dell'Autorità stessa.

"L'art. 30 del Regolamento (EU) 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 (specificatamente individuate dall'art. 30 del RGPD) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento (sul registro del responsabile, vedi, in particolare, il punto 6).

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".

2. Chi è tenuto a redigerlo?

Di estremo interesse anche la FAQ n. 2 *Chi è tenuto a redigerlo?* relativa ai soggetti tenuti a redigere il Registro del trattamento.

L'art. 30 del GDPR costruisce l'obbligo di tenuta del Registro dei trattamenti prevedendo, al primo comma, un'estensione a tutti i titolari e a tutti i responsabili del trattamento, salvo poi, all'ultimo comma, escluderne l'obbligo per ***"****imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo* 10".

Coerentemente all'impianto normativo, pertanto, il Garante prevede che siano **obbligati alla tenuta del Registro dei trattamenti**:

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 GDPR, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10 GDPR.

E' chiaro che le ipotesi che restano "scoperte" dall'obbligo di tenuta del Registro dei trattamenti siano veramente limitate e, comunque, anche in quei casi (ossia nelle ipotesi in cui la tenuta del Registro dei trattamenti non sia obbligatoria) il Garante suggerisce caldamente di istituirlo e tenerlo aggiornato in quanto il Registro dei trattamenti ***"****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".*

Interessanti sono, inoltre, le esemplificazioni fatte dal Garante circa i soggetti obbligati alla tenuta del Registro dei trattamenti tra i quali si indicano:

- 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.);

- 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);
- 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);
- 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).

Si intravedono, inoltre, i primi germogli di un'attività di semplificazione ad opera del Garante soprattutto per quanto riguarda il Registro dei trattamenti tenuti da imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del Registro.

A tal proposito, infatti, si precisa che le imprese e le organizzazioni con meno di 250 dipendenti obbligate alla tenuta del Registro potranno beneficiare di alcune misure di semplificazione nel senso che l'obbligo di redazione del Registro sarà circoscritto alle sole attività di trattamento in precedenza individuate. Ad esempio, qualora l'obbligo di tenuta del Registro discenda, all'impresa, dall'avere un solo dipendente allora il Registro del trattamento potrà essere predisposto e aggiornato esclusivamente con riferimento alla tipologia di trattamento relativo al rapporto lavorativo con l'unico dipendente dell'impresa.

Di seguito il testo della FAQ n. 2 *Chi è tenuto a redigerlo?* predisposta dall'Autorità Garante per la protezione dei dati personali pubblicata l'8 Ottobre 2018 sul sito dell'Autorità stessa.

"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:

imprese o 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.

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

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

- 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.);

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);

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);

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).

Infine, si precisa che le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del registro alle sole 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).

Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda 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.

Si invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) reperibile al seguente link: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045".

3. Quali informazioni deve contenere?

Dal punto di vista contenutistico la FAQ n. 3, *Quali informazioni deve contenere?* esplicita il contenuto già dettagliato dei primi due commi dell'art. 30 GDPR. In particolare, si evidenzia che nel campo "**finalità del trattamento**" (previsto dall'art. 30, par. 1, lett. b, GDPR) sarebbe opportuno indicare oltre alle singole specifiche finalità del 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) anche la base giuridica che legittima il trattamento.

Il riferimento, per quanto riguarda la **base giuridica del trattamento**, corre all'art. 6 del GDPR.

Nel caso in cui la base giuridica sia rappresentata dal "legittimo interesse" (art. 6, par. 1, lett. f, GDPR) sarà opportuno - specifica ulteriormente il Garante - indicare anche una descrizione del legittimo interesse perseguito, le "garanzie adeguate" eventualmente adottate e, infine, ove sia stata effettuata, la valutazione d'impatto (DPIA) eseguita dal titolare del trattamento.

La FAQ in esame, inoltre, specifica ulteriormente i concetti di "descrizione delle categorie di interessati e delle categorie di dati personali", "categorie di destinatari a cui i dati sono stati o saranno comunicati", "trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale" e, infine, di "descrizione generale delle misure di sicurezza".

Alcune osservazioni possono svolgersi con riferimento alla definizione del punto relativo a "**categorie di destinatari a cui i dati sono stati o saranno comunicati**".

In tale categoria, infatti, il Garante dispone debbano essere indicati sia gli altri titolari ai quali i dati siano comunicati (e si propone l'esempio degli enti previdenziali ai quali i dati personali dei dipendenti debbano essere necessariamente trasmessi per adempiere agli obblighi contributivi), ma anche gli altri soggetti - siano essi responsabili o sub-responsabili (di cui all'art. 28 GDPR) - ai quali il titolare trasmetta i dati personali. L'aspetto rilevante è, a questo punto, che il Garante ricomprende i soggetti esterni cui il titolare affidi il "servizio di elaborazione delle buste paga dei dipendenti" (o gli altri soggetti esterni cui siano affidate in tutto o in parte le attività di trattamento) nella categoria di responsabili o sub-responsabili del trattamento. Nella FAQ, in sostanza, si distingue nettamente tra soggetti ai quali il titolare debba necessariamente trasmettere dati personali dei propri dipendenti (enti previdenziali) da altri soggetti che trattano i dati, per conto del titolare, in forza di un accordo (previsto dall'art. 28 del GDPR).

Ciò dovrebbe servire a fugare i dubbi sollevati dalla circolare 1150 del 23 luglio 2018 del Consiglio Nazionale dell'Ordine dei Consulenti del Lavoro circa il ruolo del consulente del lavoro come titolare autonomo, "co-titolare" o responsabile "esterno" del trattamento.

N.B. Misure semplificate

Come già si è avuto modo di rilevare, le imprese e organizzazioni con meno di 250 dipendenti obbligate alla tenuta del Registro potranno comunque beneficiare di alcune misure di semplificazione, potendo circoscrivere l'obbligo di redazione del Registro alle sole 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). Sul punto si rinvia al modello di "Registro semplificato" *infra*.

Di seguito il testo della FAQ n. 3 *Quali informazioni deve contenere?* predisposta dall'Autorità Garante per la protezione dei dati personali pubblicata l'8 Ottobre 2018 sul sito dell'Autorità stessa.

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

Con riferimento ai contenuti si rappresenta quanto segue:

a) *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;*

b) *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.);*

c) *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;*

d) *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.);*

e) *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");*

f) *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.)".

4. Può contenere informazioni ulteriori?

Sempre con riferimento ai contenuti, con la FAQ n. 4 il Garante prevede la possibilità di alimentare il Registro dei trattamenti con una serie ulteriori di informazioni utili a soddisfare, appunto, le finalità dello stesso Registro.

Di seguito il testo della FAQ n. 4 *Può contenere informazioni ulteriori?* predisposta dall'Autorità Garante per la protezione dei dati personali pubblicata l'8 Ottobre 2018 sul sito dell'Autorità stessa.

"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.)".

5. Quali sono le modalità di conservazione e di aggiornamento?

Con la FAQ n. 5 l'Autorità provvede a chiarire che 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.

Di seguito il testo della FAQ n. 4 *Può contenere informazioni ulteriori?* predisposta dall'Autorità Garante per la protezione dei dati personali pubblicata l'8 Ottobre 2018 sul sito dell'Autorità stessa.

"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"

6. Che cos'è il Registro del responsabile?

Per quanto riguarda la FAQ n. 6, *Che cos'è il Registro del responsabile,* infine, relativa al Registro del responsabile del trattamento (art. 30, par. 2, GDPR) si evidenzia la necessità di tenere distinti i trattamenti per conto di ciascun titolare del trattamento. Si potrà, pertanto, tenere un unico Registro del trattamento come responsabile ma il Registro dovrà tenere ben distinte le informazioni previste dal secondo paragrafo dell'art. 30 GDPR per ciascun titolare per conto del quale i dati siano trattati.

Le FAQ del Garante, che si chiudono proponendo due differenti modelli di Registro dei trattamenti (per il titolare del trattamento e per i responsabili del trattamento), sono indubbiamente un ottimo elemento di ulteriore esemplificazione degli obblighi nascenti dall'art. 30 del GDPR.

Di seguito il testo della FAQ n. 6 *Che cos'è il Registro del responsabile?* predisposta dall'Autorità Garante per la protezione dei dati personali pubblicata l'8 Ottobre 2018 sul sito dell'Autorità stessa.

"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;*

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".*

7. Schema relativo a informazioni che il Registro dei trattamenti deve contenere

Il Registro deve contenere le seguenti informazioni	
Art. 30 Reg. 679/2016	Indicazioni del Garante privacy
Il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati	//
Le finalità del trattamento	Es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro, e/o trattamento dei dati di contatto dei fornitori per la gestione degli ordini nonché, l'indicazione della base giuridica del trattamento
Una descrizione delle categorie di interessati e delle categorie di dati personali	Es. clienti, fornitori, dipendenti - dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.
Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali	Es. enti previdenziali
Se 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	//
Se possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati	Ad es. "in caso di rapporto contrattuale, i dati saranno conservati per 10 anni dall'ultima registrazione
Se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative	Qui andranno indicate le misure adottate in base all'art. 32 del reg. quali la pseudonimizzazione, i sistemi di ripristino in caso di interruzioni o sospensioni dell'accesso ai dati, le procedure in atto per testare le misure di sicurezza in atto

8. Modello di "Registro semplificato" delle attività di trattamento del titolare per PMI

MODELLO DI "REGISTRO SEMPLIFICATO" DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE PER PMI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*							
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*							
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*							
TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

9. Modello di "Registro semplificato" delle attività di trattamento del responsabile per PMI

MODELLO DI "REGISTRO SEMPLIFICATO" DELLE ATTIVITÀ DI TRATTAMENTO DEL RESPONSABILE PER PMI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI DEL RESPONSABILE/SUB-RESPONSABILE *[per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]*		
RESPONSABILE *[inserire la denominazione e i dati di contatto]*		
TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*		
RESPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*		
CATEGORIA DI TRATTAMENTO	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE


FLA
FEDERLEGNOARREDO