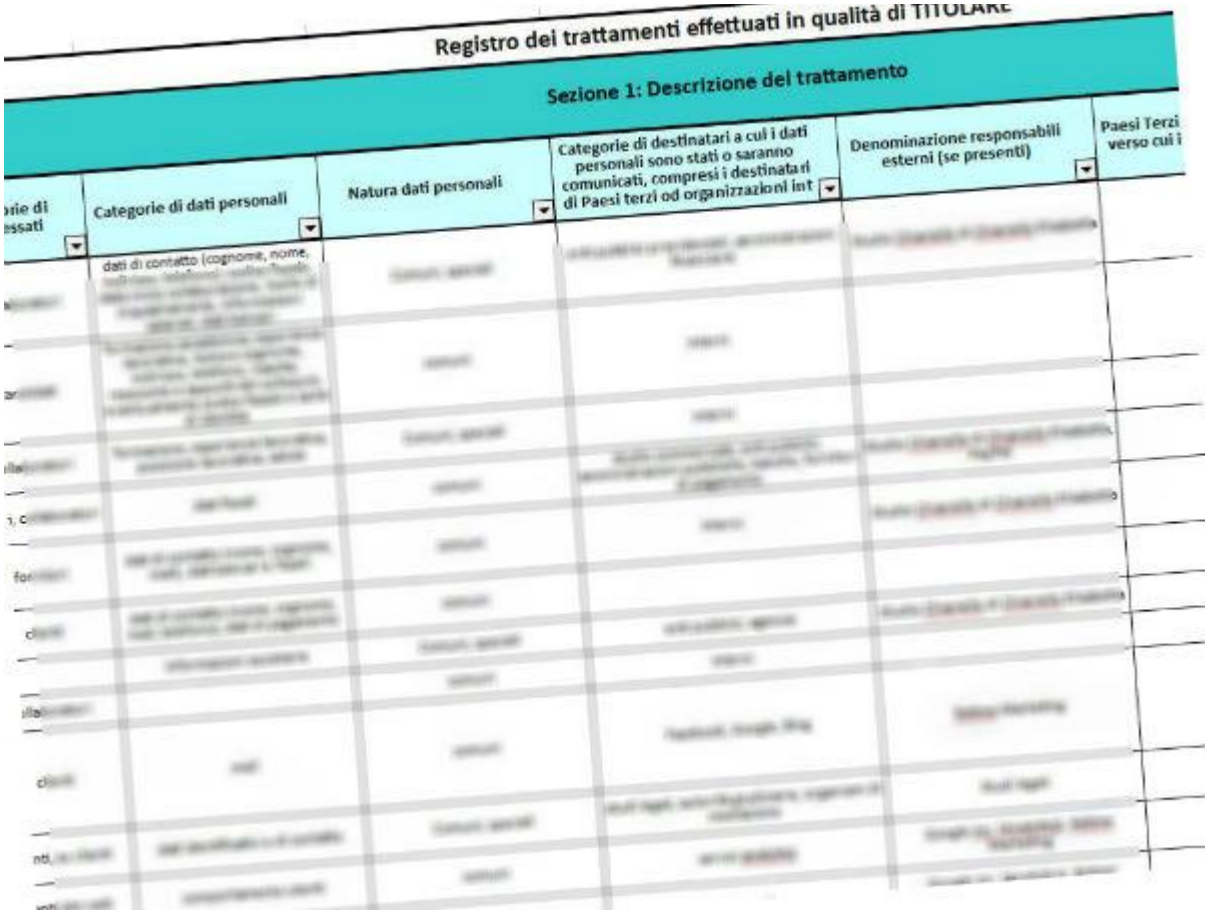
https://protezionedatipersonali.it/registro-dei-trattamenti, 17-11-2018

Registro dei trattamenti



La tenuta del **registro dei trattamenti** è prevista dall'articolo 30 del regolamento generale europeo, ed è considerata indice di una corretta gestione dei trattamenti.
L'onere della tenuta del registro è a carico del titolare e, se nominato,
del responsabile del trattamento. La tenuta del registro costituisce uno dei principali elementi di accountability del titolare, in quanto è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzato anche all'analisi del rischio e ad una corretta pianificazione dei trattamenti. Per cui le autorità invitano tutti i titolari a dotarsene, eventualmente inserendo nel registro ogni elemento utile, anche oltre a quelli minimi previsti dalle norme.
Il registro deve essere tenuto in **forma scritta, anche in formato elettronico**, e va esibito all'autorità di controllo (Garante) in caso di verifiche. Ovviamente il registro deve essere costantemente aggiornato. il registro deve anche recare "in maniera verificabile" sia la **data della sua prima istituzione** o creazione sia la **data dell'ultimo aggiornamento**.

Registro dei titolari del trattamento

Il registro deve elencare una serie di informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, se nominati, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (DPO);
b) le finalità del trattamento, 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);
c) una descrizione delle categorie di interessati (es. clienti, fornitori, dipendenti) e delle categorie dei dati personali (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.);
d) le categorie di destinatari (anche solo per categoria di appartenenza) a cui i dati personali sono stati o saranno comunicati (compreso gli altri titolari, come gli enti previdenziali, ma è opportuno indicare anche i responsabili e sub-responsabili ai quali sono trasmessi i dati, come i soggetti ai quali il titolare affidi il servizio di elaborazione delle buste paga dei dipendenti);
e) ove 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;
f) dove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) dove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 (è possibile fare riferimento a documenti esterni).
Quali ulteriori elementi si suggerisce di inserire la base giuridica del trattamento. Nel caso di trattamento basato sui legittimi interessi si consiglia di 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. Per i trattamenti di dati di cui all'art. 9 del GDPR, è opportuno indicare una delle condizioni di cui all'art. 9, par. 2. In caso di trattamenti di dati relativi a condanne penali e reati, si consiglia di riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'art. 10 del regolamento europeo.

Registro dei responsabili del trattamento

Il paragrafo 2 dell'articolo 30 del GDPR prevede che anche i responsabili del trattamento debbano tenere un registro simile in relazione alle attività svolte per conto del titolare. Il contenuto deve essere il seguente:
- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- ove 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;

- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Esenzioni

Sono **esentate dall'obbligo di tenuta del registro le imprese o le organizzazioni con meno di 250 dipendenti**, a meno che il trattamento effettuato:
- possa presentare un rischio (anche non elevato) per i diritti e le libertà degli interessati,
- 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 (cioé dati sensibili o giudiziari).

In tale prospettiva l'autorità di controllo italiana nelle sue linee guida precisa che rientrano nell'obbligo di tenuta del registro:
- **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).

In tema di semplificazioni, l'autorità di controllo precisa che le imprese e le organizzazioni con meno di 250 dipendenti ma che comunque sono obbligate alla tenuta del registro potranno limitarsi a inserire nel registro le sole attività di trattamento che fanno scattare l'obbligo del registro.

Parere del Gruppo Articolo 29

Il Working Party Article 29 (ora EDPB) ha pubblicato un parere sul registro dei trattamenti (qui il link al parere), nel quale precisa che **è sufficiente che occorra una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro**. Per cui basta trattare dati personali in modo stabile per essere tenuti alla registrazione dei trattamenti.

In tale prospettiva occorre ricordare che qualsiasi azienda tratta dati sensibili (relativi alla salute) dei propri dipendenti (ad esempio, un'aspettativa per motivi di salute). Anche i liberi professionisti trattano dati personali altrui in maniera non occasionale. Ed anche un sito web con un form di contatti.

Il parere del WP29 chiarisce che è sufficiente registrare i soli trattamenti che attivano l'obbligo di tenuta, e invitano le Autorità nazionali a proporre sui propri siti un modello di registro semplificato per le piccole e medie imprese.