

Documento	REGISTRO DEI TRATTAMENTI - AUDIT
Adempimenti	ART. 30 REG.679/16 – Versione del Titolare
Documenti relati	INDEX679, SOP3_3, DT679, PolPP, RDTA, DVR/IP
Riferimenti	Piano di adeguamento 2023-24

CONTENUTI

- Politica del Titolare del Trattamento (**TDT**)
- Adempimenti congiunti per eventuale Responsabile del Trattamento (**RDT**)
- Lista controlli operativi del Registro (versione Titolare)
- Istruzioni di post compilazione per modulistica Manuale del SPPD

La Azienda è consapevole che l'Art. 30 del GDPR (Regolamento europeo in materia di protezione dei dati personali) riguarda uno degli adempimenti più importanti concernenti le attività di trattamento dei dati personali.

Secondo il par. 4 dell'art. 30, *“su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.”*

Pertanto è recepito dal Titolare l'obbligo di documentazione della conformità della propria organizzazione alle prescrizioni della legge. Tale diligenza grava congiuntamente anche sul Responsabile, per i trattamenti svolti per conto del Titolare.

L'autorità di controllo (Garante e Nucleo investigativo deputato della GdF (**GAT**)) hanno titolo per richiedere la disponibilità del registro, al fine di esaminarlo.

L'obbligo di detenere un **RDT** non è assoluto, infatti il *par. 5 dell'art. 30* specifica che esso non compete *“alle 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”*; tuttavia la nostra azienda ha seguito una valutazione sistematica orientata ai rischi producendo comunque la presente lista di riscontro relativa al RDT.

Le finalità del TDT sono:

- A) rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;
- B) costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

ISTRUZIONI: una volta compilato e validato con data e firme dei soggetti responsabili, il documento è scandito e riprodotto in vetrofania, bacheca e/o manuale digitale del SPPD aziendale secondo politiche Privacy e/o Istruzioni operative preordinate in fase di Valutazione dei Rischi e Degli Impatti

- TITOLARE
- RESPONSABILE
- TEAM DI LAVORO
- ADS / DBA



[Documentazione di Sistema] [Piano di Adeguamento] Sez.Proc. Gestionali e Operative

SPPD

Framework

M.S.P.

PIANO DI AUDIT REGISTRO TRATTAMENTI – VERSIONE TITOLARE DEL TRATTAMENTO

N. REQUISITO PER ADEMPIENZA

1 L'organizzazione ha un numero di dipendenti pari o superiore a 250?

SI NO NA

NOTE :

.....

.....

2 Sono effettuati trattamenti che possono presentare un rischio per i diritti e le libertà degli interessati?

SI NO NA

NOTE :

.....

.....

3 In caso di risposta negativa al quesito n. 1) ma affermativa al n. 2), il trattamento è occasionale?

SI NO NA

NOTE :

.....

.....

4 In caso di risposta negativa al quesito n. 1) ma affermativa al n. 2), il trattamento include "categorie particolari di dati di cui all'articolo 9, paragrafo 1 (che sono gli odierni dati sensibili, con l'aggiunta dei dati genetici e biometrici), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10"?

SI NO NA

NOTE :

.....

.....

5 Contiene il registro il nome e i dati di contatto del titolare del trattamento?

SI NO NA

NOTE :

.....

.....

6 Sono indicati il nome e i dati di contratto, ove sussistenti:

...del contitolare del trattamento?
...del rappresentante del titolare del trattamento?
...del responsabile della protezione dei dati?

SI NO NA

NOTE :

.....

.....

7 Sono esplicitate le finalità dei trattamenti effettuati?

SI NO NA

NOTE :

.....

.....

8 Per ciascun trattamento sono individuate le categorie di interessati (ad es., dipendenti, clienti/utenti, fornitori, ecc.)?

SI NO NA

NOTE :

.....

.....

9 Per ciascun trattamento sono individuate le categorie di dati, sono cioè rintracciati:

- dati che rivelano l'origine razziale o etnica (art. 9)?*
- dati che rivelano le opinioni politiche (art. 9)?*
- dati che rivelano le convinzioni religiose o filosofiche (art. 9)?*
- dati che rivelano l'appartenenza sindacale (art. 9)?*
- dati genetici (artt. 4, par. 1, n. 13 e 9)?*
- dati biometrici (artt. 4, par. 1, n. 14 e 9)?*
- dati relativi alla salute (artt. 4, par. 1, n. 15 e 9)?*
- dati relativi alla vita/orientamento sessuale (art. 9)?*
- dati relativi a condanne penali e reati (art. 10)?*

SI NO NA

NOTE :

.....

.....

10 Per ciascun trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?

SI NO NA

NOTE :

.....

.....

11 Vi sono trattamenti in cui i dati sono comunicati a destinatari di Paesi terzi ovvero di organizzazioni internazionali?

SI NO NA

NOTE :

.....

.....

12 Contiene il registro l'indicazione dei trattamenti che includono i trasferimenti di dati personali verso un paese Terzo o un'organizzazione internazionale?

SI NO NA

NOTE :
.....
.....

13 In caso di risposta affermativa al quesito n. 12), il registro include l'identificazione del paese terzo o dell'organizzazione internazionale?

SI NO NA

NOTE :
.....
.....

14 In caso di risposta affermativa al quesito n. 11), per i trasferimenti di cui al secondo comma dell'articolo 49, il registro documenta le prescritte garanzie adeguate (per l'art. 49, comma 2, "Il trasferimento di cui al paragrafo 1, primo comma, lettera g) [che sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse], non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari?)

SI NO NA

NOTE :
.....
.....

15 E' individuata la base giuridica (ad es., contratto, legge, standard internazionale, ecc.) di ciascun trattamento?

SI NO NA

NOTE :
.....
.....

16 **Detta base giuridica consente, per ciascun trattamento, di definire un tempo massimo di gestione/conservazione dei dati?**

SI NO NA

NOTE :
.....
.....

17 **Sono indicati i termini ultimi previsti per la cancellazione delle diverse categorie di dati?**

SI NO NA

NOTE :
.....
.....

18 **Sono descritte le misure di sicurezza tecniche e quelle organizzative di cui all'articolo 32, par. 1, tra cui, a titolo di esempio:**

- *la pseudonimizzazione e la cifratura dei dati personali?*
la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?
la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico?
una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?

SI NO NA

NOTE :
.....
.....

19 **Dette misure garantiscono un livello di sicurezza adeguato al rischio?**

SI NO NA

NOTE :
.....
.....

20 Ha il titolare aderito ad un codice di condotta (art. 40) o ad un sistema di certificazione (art. 42)?

SI NO NA

NOTE :
.....
.....

21 In quale misura il detto codice di condotta/sistema di certificazione include adempimenti in materia di misure di sicurezza dei trattamenti?

SI NO NA

NOTE :
.....
.....

22 Il registro contiene l'informazione circa l'adesione del titolare al codice di condotta/sistema di certificazione?

SI NO NA

NOTE :
.....
.....

23 Esplicita il registro le misure tecniche ed organizzative implementate e riconducibili al codice di condotta e/o al sistema di certificazione

SI NO NA

NOTE :
.....
.....

24 Reca il registro la data della sua emissione?

SI NO NA

NOTE :
.....
.....

25 E' specificato se si tratta di prima emissione o di successiva revisione?

SI

NO

NA

NOTE :
.....
.....

26 E', il registro, sottoscritto dalla funzione che in base al sistema di procure e deleghe dell'organizzazione è deputata a farlo?

SI

NO

NA

NOTE :
.....
.....

27 E' stabilita la modalità di conservazione del registro?

SI

NO

NA

NOTE :
.....
.....

28 E' definito l'ambito di distribuzione interna del registro?

SI

NO

NA

NOTE :
.....
.....

29 E' individuata la funzione responsabile della conservazione e distribuzione interna del registro?

SI

NO

NA

NOTE :
.....
.....

30 Il titolare ha pianificato la revisione del registro?

SI

NO

NA

NOTE :

.....

.....

SPPD

Framework

MSP