

Allegato 2

ISTRUZIONI SULLE MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI PER I DESIGNATI A SPECIFICI COMPITI E FUNZIONI AI SENSI DELL'ARTICOLO 29 DEL GDPR E DELL'ARTICOLO 2-QUATERDECIES DEL CODICE PRIVACY

L'ARERA con il presente documento intende fornire ai Designati di primo e di secondo livello, preposti ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy allo svolgimento di specifici compiti e funzioni per i trattamenti di dati personali svolti nell'ambito della unità organizzativa di riferimento, le istruzioni cui attenersi, unitamente alle Istruzioni di cui all'Allegato 1, nello svolgimento degli specifici compiti e funzioni loro delegati.

Nell'esecuzione dei compiti attribuiti ogni Designato di secondo livello deve coinvolgere il Designato di primo livello di riferimento e il RPD, anche al fine di acquisire eventuali chiarimenti, attenendosi alle sue indicazioni o motivando eventuali decisioni difformi.

1. CENSIMENTO PERIODICO DEI TRATTAMENTI

L'articolo 30 del GDPR prevede, tra gli adempimenti principali del Titolare del trattamento, la tenuta del "Registro dei trattamenti" nel quale devono essere riportate le principali informazioni relative alle operazioni di trattamento svolte dal Titolare.

Il Registro 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 dei trattamenti è un documento di censimento e analisi dei trattamenti effettuati e 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.

Per ogni trattamento, il Designato di secondo livello deve comunicare al RPD e, per conoscenza, al Designato di primo livello, o quest'ultimo direttamente al RPD, almeno le seguenti informazioni:

- a. descrizione del trattamento;
- b. finalità del trattamento;
- c. tipologie di operazioni svolte sui dati (ad esempio acquisizione, elaborazione, conservazione);
- d. eventuale presenza di soggetto contitolare dei dati ai sensi dell'articolo 26 del GDPR;
- e. eventuale presenza di soggetto responsabile del trattamento dei dati ai sensi dell'articolo 28 del GDPR;
- f. tipologia dati personali (comuni, particolari, giudiziari) e relativa base giuridica del trattamento;

Allegato 2

- g. tempo di conservazione del dato: per ogni trattamento deve essere individuato il tempo di cancellazione per tipologia e finalità di trattamento o, ove non sia possibile stabilire a priori un termine massimo, i criteri usati per determinare tale periodo (ad es. norme di legge);
 - h. volume del dato: indicare una stima quantitativa dei dati trattati nell'ambito del trattamento;
 - i. categoria interessati: utenti, dipendenti, operatori;
 - j. eventuali categorie di destinatari a cui i dati sono stati o saranno comunicati (ad es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi);
 - k. eventuale trasferimento dei dati in Paesi terzi;
 - l. misure di sicurezza organizzative adottate.
- Inoltre, con il supporto del Responsabile SIN, devono essere comunicati:
- a. *asset* impiegati nel trattamento (hardware diverso dai pc assegnati ai dipendenti);
 - b. minacce agli *asset*;
 - c. misure di sicurezza tecnica adottate.

2. VALUTAZIONE DI IMPATTO SUL TRATTAMENTO DI DATI

Ai sensi dell'articolo 35 del GDPR, quando viene avviato un nuovo trattamento, specie se questo prevede l'uso di nuove tecnologie, o se vengono modificate le modalità di un trattamento preesistente, anche in relazione agli strumenti impiegati per lo svolgimento dello stesso, il Titolare del trattamento è obbligato a effettuare, prima di procedere al trattamento o di modificarne le caratteristiche, una valutazione di impatto sulla protezione dei dati (o *Data Protection Impact Assessment*, di seguito: DPIA).

La DPIA è svolta dal Designato di primo livello e, ove presente, dal Designato di secondo livello, che deve obbligatoriamente acquisire il parere del RPD.

Al fine dello svolgimento di tale procedura, la cui omissione è punita, ai sensi dell'articolo 83 del GDPR, con sanzione fino a 10 milioni di euro, devono essere forniti dai Designati al RPD tutti i dati previsti per il censimento del trattamento.

Le informazioni devono essere fornite dai Designati anche qualora ritengano che non sussista l'obbligo di svolgimento della DPIA ai sensi del paragrafo 3 del richiamato articolo 35 del GDPR.

3. COORDINAMENTO E FORMAZIONE DEGLI AUTORIZZATI

I Designati possono delimitare le autorizzazioni dei dipendenti assegnati alla propria unità organizzativa rispetto agli specifici trattamenti censiti nell'unità organizzativa, mediante il modello A allegato alle presenti Istruzioni. Tale delimitazione deve corrispondere ai trattamenti che i dipendenti sono abilitati a svolgere mediante i sistemi informativi preposti.

I Designati sono tenuti a verificare il rispetto, da parte degli autorizzati assegnati all'unità organizzativa di appartenenza, delle istruzioni di cui all'Allegato 1 del Regolamento Privacy.

Nell'ambito di tale attività, i Designati di primo sono tenuti ad acquisire il censimento dei fabbisogni formativi specifici in materia di trattamento dei dati dei dipendenti effettuato dai Designati di secondo livello e ad inviare al RPD e alla Direzione Affari Generali e Risorse il fabbisogno formativo complessivo entro il 30 giugno di ciascun anno.

Allegato 2

4. OBBLIGO DI FORMAZIONE E AGGIORNAMENTO

I Designati di primo e di secondo livello sono tenuti a partecipare attivamente e in prima persona, nonché a favorire la partecipazione dei Referenti *privacy* e di tutti i dipendenti alle iniziative formative loro dedicate e a studiare il materiale informativo messo a disposizione da ARERA anche tramite la sezione dedicata presente sul sito *intranet*.

Allegato 2

Allegato 2, modello A

**MODELLO DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI AI SENSI
DELL'ARTICOLO 29 DEL REGOLAMENTO (UE) 2016/679 (GDPR) E DELL'ARTICOLO 2-
QUATERDECIES DEL D.LGS. N. 196/2003**

L'Autorità di Regolazione per Energia Reti e Ambiente, con sede a Milano, Piazza Cavour n. 5, in qualità di Titolare del trattamento dei dati (di seguito: Titolare o ARERA), in persona del/della dott./dott.ssa [●], Direttore della Divisione/Direzione/Responsabile dell'Ufficio speciale di Sua assegnazione, in forza della designazione allo svolgimento di specifici compiti e funzioni per i trattamenti di dati personali svolti nell'ambito della Direzione/dell'Ufficio di appartenenza di cui al Regolamento dell'Autorità di Regolazione per Energia Reti e Ambiente relativo agli adempimenti in materia di trattamento dei dati personali ai sensi dell'articolo 29 del Regolamento (UE) n. 2016/679 e dell'articolo 2-*quaterdecies* del decreto legislativo 30 giugno 2003, n. 196 (di seguito: Regolamento Privacy, allegato A alla deliberazione 362/2024/A),

AUTORIZZA

[Nome] [Cognome], [Qualifica] della Divisione/Direzione/dell'Ufficio predetta/o (di seguito: Autorizzato), a trattare, anche per il tramite dei sistemi informativi gestionali a ciò preposti, i dati personali di cui ai seguenti trattamenti, come indicati nel registro dei trattamenti di ARERA:

- a) [●];
- b) [●];
- c) [●].

A tal fine l'Autorizzato si obbliga a osservare gli obblighi e le istruzioni di cui al Regolamento Privacy.

La presente autorizzazione sostituisce quella più generale di cui all'articolo 4 del Regolamento Privacy.

Milano/Roma, [●]

Firma