Allegato A

Istruzioni per i Direttori designati al trattamento dei dati personali

Premessa

L'Autorità di Regolazione per Energia Reti e Ambiente, Titolare del trattamento dei dati personali, ha attribuito con la deliberazione 356/2019/A ai Dirigenti responsabili della Macrostruttura (Segretario Generale, Direttore di Divisione, Direttore di Direzione, Responsabile di Ufficio speciale), ciascuno per i procedimenti e le attività di competenza, come assegnati dal Regolamento di organizzazione e funzionamento dell'Autorità, gli specifici compiti e funzioni connessi al trattamento dei dati personali di cui al Regolamento UE 2016/679 (di seguito: GDPR), in attuazione dell'articolo 2 – *quaterdecies* del D. Lgs 10 agosto 2018, n. 101 di modifica del D.lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" (di seguito: Codice Privacy).

Nel richiamare preliminarmente la documentazione presente nella pagina del sito Intranet (Organizzazione e Personale → Privacy) dove sono riportate le circolari e le procedure in uso già approvate dal Collegio (in particolare le *"Linee guida e regole operative n.1 del 25/5/2018"*), si informa che per consulenza e supporto occorre rivolgersi al Responsabile della Protezione dei Dati personali dell'Autorità (di seguito: RPD), dottoressa Patrizia Cardillo, che può essere contattata al numero 0669791442 oppure all'indirizzo: rpd@arera.it.

Nel seguito si riportano, in sintesi, le definizioni, i principi generali, le principali misure di sicurezza e le istruzioni cui i Designati dovranno attenersi per il corretto trattamento dei dati personali e di cui dovranno dare massima diffusione tra i propri collaboratori anche non autorizzati ai trattamenti.

1. Ambito di applicazione e definizioni

Il GDPR si applica al trattamento interamente o parzialmente automatizzato di dati personali ed al trattamento non automatizzato di dati personali, contenuti negli archivi dell'Autorità. Ne consegue che tutto il personale dell'Autorità si troverà a trattare dati personali.

Con il termine «**trattamento**» il GDPR individua "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi*

altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Con il termine «**dato personale**» si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Finalità della disciplina in materia di privacy è la tutela del diritto fondamentale dell'individuo alla protezione dei propri dati personali ed obiettivo del Titolare sarà quello di adottare e mettere in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR.

2. Principi generali

Nel trattare i dati personali ogni Direttore designato dovrà attenersi ai principi generali contenuti nell'art. 5 del GDPR.

In particolare, i dati personali devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
    - ✓ *Ogni trattamento deve trovare fondamento in un'idonea base giuridica (ad esempio: il consenso prestato per finalità specifiche, un contratto, adempimento di obblighi, esercizio di pubblico potere, fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici) e deve garantirsi all'interessato l'accesso ad alcune informazioni anche per mettere l'interessato nelle condizioni di esercitare i propri diritti*
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
    - ✓ *Occorre quindi coerenza con la finalità per cui il dato è trattato e limitarsi alla raccolta del dato strettamente necessario alla finalità (ad esempio: nella gestione del rapporto di lavoro saranno richiesti e trattati molti più dati che non nel riscontrare un'istanza di accesso agli atti di persona esterna)*
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati, nel rispetto del principio di minimizzazione e di limitazione delle finalità;
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati in attuazione del principio di limitazione della conservazione.
    - ✓ *Una volta conseguita la finalità, i dati possono essere cancellati salvo che residuino altre finalità, ad esempio che vengano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali compresa la protezione con misure tecniche ed organizzative, in modo da garantire riservatezza e integrità.
    - ✓ *Vista la numerosità delle informazioni presenti negli archivi, per questo aspetto si rimanda alla policy adottata dall'Autorità con gli atti pubblicati sulla pagina Privacy di intranet (https://intranet.arera.it/intranet/page/privacy) chiedendo di prestare particolare attenzione alle "**Linee guida e regole operative n.1 del 25/5/2018**", "**Disposizioni per il corretto utilizzo delle risorse informatiche e telematiche**" ed all' "**Information Security Policy per i fornitori**". Le stesse devono essere trasmesse ai propri collaboratori che si trovano a trattare il dato personale nell'ambito del rapporto di lavoro.*

****

3. MISURE DI SICUREZZA

Nella sezione Privacy di intranet (*https://intranet.arera.it/intranet/page/privacy*) sono riportate le linee guida, le istruzioni e le prime misure di sicurezza adottate dall'Autorità, Titolare del trattamento, per le diverse tipologie di trattamenti posti in essere, distinte in base alle modalità con cui il trattamento è realizzato (cartaceo/strumenti elettronici). Si richiamano in particolare le "Linee guida e regole operative n.1 del 25/5/2018", "Disposizioni per il corretto utilizzo delle risorse informatiche e telematiche" ed all' "Information Security Policy per i fornitori". In base a quanto previsto dal GDPR tali misure dovranno essere sempre aggiornate tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

Fermo quanto previsto in via generale, ai Designati ed al personale che opera sul trattamento dei dati personali, ognuno per i trattamenti di competenza, è fatto divieto:

- di comunicare e diffondere con qualsiasi mezzo i dati personali oggetto di trattamento ad altri lavoratori a qualsiasi titolo presenti in Autorità;

- di comunicare e diffondere con qualsiasi mezzo i dati personali oggetto di trattamento a soggetti terzi che non siano stati preventivamente autorizzati dall'Autorità.

Si intende per:

a. "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
b. "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (Art. 2-*ter* del Codice privacy).

3.1. Misure di sicurezza in caso di trattamenti cartacei

Premesso che l'Autorità mette a disposizione di tutti i lavoratori strumenti informatici volti a ridurre al minimo i trattamenti dei dati personali con modalità cartacee, eventuali copie analogiche di un documento dovranno essere:

a) custodite in modo da evitare che terzi possano accedervi anche in modo casuale;
b) in particolare, non abbandonate nelle stampanti comuni o su tavoli comuni;
c) non divulgate; come sopra si è già espressamente fatto divieto, il contenuto delle copie non deve essere diffuso al di fuori delle ipotesi in cui ciò è espressamente richiesto;
d) distrutte al termine del procedimento o dell'attività salvo diverso obbligo di archiviazione per finalità di legge.

3.2. Misure di sicurezza in caso di trattamenti elettronici

Nell'ambito dei trattamenti operati tramite i sistemi informativi, ferme restando le previsioni della più volte citata circolare DSIL n.2/2014 relativa a "*Disposizioni per il corretto utilizzo delle risorse informatiche e telematiche*", tutti sono tenuti in particolare a:

a) utilizzare esclusivamente i sistemi informativi, nonché i terminali e i software messi a disposizione dall'Autorità o da questa approvati e attenersi alle istruzioni impartite;
b) custodire con cura e diligenza le proprie credenziali per l'accesso e l'utilizzo dei sistemi informativi;

c) non cedere o divulgare le proprie credenziali per l'accesso e l'utilizzo dei sistemi informativi;
d) aggiornare almeno ogni tre mesi la password di accesso ai sistemi informativi;
e) non utilizzare sistemi di memorizzazione automatica delle credenziali di accesso, specie nell'ipotesi in cui venga utilizzato un terminale di proprietà;
f) non lasciare incustodito e/o liberamente accessibile, anche se all'interno dei locali dell'Autorità, il terminale tramite il quale sta svolgendo il trattamento;
g) evitare l'invio di messaggi di posta elettronica con documenti che contengono dati personali;
h) non realizzare backup dei dati su supporti o terminali di proprietà.

4. ISTRUZIONI OPERATIVE

In particolare, ogni Direttore designato, attraverso i suoi Referenti privacy, dovrà:

a) aggiornare il Registro dei trattamenti della propria Macrostruttura in particolare nei casi di avvio di nuovi trattamenti, di variazione di soggetti autorizzati, di variazione di modalità o di misure di sicurezza; la copia aggiornata dovrà essere trasmessa tempestivamente al RPD che tiene il Registro dei Trattamenti dell'Autorità;
b) individuare e autorizzare i propri collaboratori che operano su ciascun trattamento, con modalità ritenute più opportune, ma comunque idonee ad assicurare il rispetto del principio di accountability;
c) informare, istruire e comunque sensibilizzare tutto il proprio personale sul tema della protezione dei dati personali; favorire la partecipazione ai corsi di formazione organizzati dall'Autorità e/o dal RPD;
d) individuare, anche congiuntamente tra loro, i Referenti privacy che hanno in compito di supportarli relativamente ai trattamenti dei dati personali;
e) segnalare al RPD casi di possibili violazioni dei dati personali trattati attenendosi alla procedura *Data Breach* già adottata dall'Autorità;
f) aggiornarsi e attenersi alle istruzioni già adottate dall'Autorità (Circolare n. 2 del 2014; Linee guida e regole operative n.1 del 25/5/2018) e a quelle che verranno adottate;
g) coinvolgere tempestivamente e adeguatamente il RPD in tutte le questioni riguardanti la protezione dei dati personali, compresi i casi in cui si evidenzi l'esigenza di avviare una preventiva valutazione di impatto nel caso in cui un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate. Eventuali scelte difformi dal parere reso dal RPD dovranno essere motivate in conformità al principio di accountability;
h) verificare, tramite i responsabili dei contratti o i direttori dell'esecuzione dei contratti, che i contratti o altri atti giuridici che disciplinano i rapporti con i rispettivi "Responsabili del Trattamento dei dati" (RTD: cioè quei soggetti

esterni all'Autorità che elaborano e trattano dati per conto del Titolare, generalmente fornitori di servizi) siano conformi a quanto previsto dall'art. 28 del GDPR. In particolare, il RTD dovrà fornire garanzie sufficienti sull'adozione di misure tecniche ed organizzative adeguate alla tipologia, durata e finalità del trattamento assegnato ed i responsabili dei contratti o i direttori dell'esecuzione dei contratti dovranno altresì monitorare e vigilare sul rispetto delle istruzioni impartite ai RTD e intervenire tempestivamente in caso di eventuale violazione;

i) segnalare al RPD e al Responsabile dei sistemi informativi i casi in cui si ritiene necessario/opportuno adottare ulteriori misure organizzative e tecniche a tutela dei dati trattati; ovvero l'esigenza di avviare preventivamente una valutazione d'impatto del trattamento;

j) in tema di richieste presentate ai sensi degli articoli da 15 a 22 del GDPR, trasmettono, ognuno per i trattamenti di competenza, le informazioni necessarie al RPD entro dieci giorni dalla richiesta dell'interessato o dello stesso RPD; devono provvedere a rispondere alle richieste degli interessati ed ai successivi eventuali adempimenti di competenza; devono, infine, segnalare tempestivamente ogni richiesta ritenuta di non competenza per la nuova assegnazione.