Allegato 3

ISTRUZIONI SULLE MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI IN QUALITÀ DI AMMINISTRATORE DI SISTEMA

L'ARERA con il presente documento intende fornire al Responsabile SIN e a tutti gli amministratori di sistema, nominati ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy e del provvedimento del 27 novembre 2008, le istruzioni cui devono attenersi nello svolgimento delle relative attività, unitamente alle Istruzioni di cui all'Allegato 1.
In caso di dubbi sull'interpretazione delle presenti istruzioni è possibile rivolgersi al Responsabile SIN, nonché al RPD.

1. OBBLIGHI DELL'AMMINISTRATORE

Ciascun soggetto nominato Amministratore di Sistema è tenuto a:

1. assegnare e gestire i codici identificativi a ciascun utente del sistema informatico prevedendone la disattivazione nel caso di cessazione dei requisiti di accesso, ovvero nel caso di mancato utilizzo per un periodo superiore a sei mesi;
2. non comunicare o diffondere i codici identificativi a un soggetto diverso dal legittimo titolare;
3. disporre ogni opportuna misura e ogni adeguata verifica per evitare che soggetti non autorizzati possano avere accesso agli archivi delle parole chiave se leggibili;
4. impiegare e non manomettere i sistemi di registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ovvero ai sistemi di trasmissione dati o di sicurezza e agli archivi elettronici;
5. segnalare tempestivamente al Designato di primo livello di riferimento, al Responsabile SIN e al RPD ogni tipo di violazione dei sistemi di registrazione degli accessi logici o di eventuale obsolescenza o criticità che ne pregiudichi la completezza e l'inalterabilità o la possibilità di verifica della loro integrità;
6. effettuare periodici *backup* dei dati e delle applicazioni e verificarne la funzionalità e utilizzabilità in caso di *disaster recovery*;
7. segnalare tempestivamente al Designato di primo livello, al Responsabile SIN e al RPD l'eventuale inadeguatezza ai sensi dell'articolo 32 del GDPR o obsolescenza di una misura di sicurezza adottata;
8. adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
9. provvedere alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego in ossequio a quanto prescritto dal Garante per la protezione dei dati personali nel provvedimento del 13 ottobre 2008;
10. comunicare tempestivamente al Designato di primo livello di riferimento, al Responsabile SIN e al RPD qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali;

11. segnalare entro 24 ore dalla scoperta al Designato di primo livello di riferimento, al Responsabile SIN e al RPD l'eventuale violazione di uno o più sistemi di ARERA, indicando, altresì, gli specifici *asset* oggetto della violazione.

2. MISURE DI SICUREZZA ADEGUATE AL TRATTAMENTO

L'ARERA definisce le misure di sicurezza adeguate alle tipologie di trattamenti posti in essere. In generale, si ricorda che Le è fatto divieto di:
a) comunicare i dati personali, il cui trattamento Le viene affidato, a dipendenti o consulenti di ARERA;
b) comunicare i dati personali, il cui trattamento Le viene affidato, a soggetti terzi che non siano stati preventivamente autorizzati da ARERA.
In qualità di Amministratore di Sistema, Lei è tenuto ad informare tempestivamente il Designato di primo livello di riferimento, il Responsabile SIN e il RPD allorquando ritenesse che una o più misure di sicurezza adottate non siano più adeguate ai rischi insiti nel trattamento dei dati personali svolto da ARERA.

Le misure di sicurezza adottate da ARERA sono distinte a seconda delle modalità con cui il trattamento è realizzato:
1) trattamenti cartacei;
2) trattamenti con l'ausilio di strumenti elettronici.

2.1. Misure di sicurezza in caso di trattamenti cartacei

ARERA ha sviluppato strumenti informativi volti a ridurre al minimo i trattamenti dei dati personali con modalità cartacee. Qualora Lei realizzi la copia analogica di un documento deve:
a) custodirla in modo da evitare che terzi possano accedervi, ad esempio non lasciandola incustodita;
b) non divulgarne il contenuto al di fuori delle ipotesi in cui ciò è espressamente richiesto;
c) distruggere la copia analogica al termine del procedimento o dell'attività.

2.2. Misure di sicurezza in caso di trattamenti elettronici

Nell'ambito dei trattamenti operati tramite i sistemi informativi, Lei è tenuto a:
a) utilizzare esclusivamente i sistemi informativi, nonché i terminali e i software messi a disposizione da ARERA o da questa approvati;
b) custodire con cura e diligenza le Sue credenziali per l'accesso e l'utilizzo dei sistemi informativi;
c) non cedere o divulgare le Sue 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 utilizzi un terminale di Sua proprietà;
f) non lasciare incustodito e/o liberamente accessibile, anche se all'interno dei locali di ARERA, 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 Sua proprietà.

3. OBBLIGO DI AGGIORNAMENTO

Ogni Amministratore di Sistema è tenuto a studiare il materiale informativo messo a disposizione da ARERA, nonché a partecipare alle attività di studio e approfondimento promosse dalla stessa.

4. SANZIONI

Il mancato rispetto da parte dell'Autorizzato delle istruzioni impartite, e degli obblighi connessi alla sua autorizzazione al trattamento dei dati personali, configura una infrazione disciplinare e potrà comportare l'avvio di un procedimento disciplinare anche nell'ipotesi in cui da ciò non discenda l'avvio di un procedimento sanzionatorio da parte del Garante per la protezione dei dati personali o non consegua la richiesta di danni da parte degli interessati al trattamento.