Allegato 1

ISTRUZIONI SULLE MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI PER GLI AUTORIZZATI AI SENSI DELL'ARTICOLO 29 DEL GDPR E DELL'ARTICOLO 2-*QUATERDECIES* DEL CODICE PRIVACY

L'ARERA con il presente documento intende fornire ai dipendenti, autorizzati al trattamento dei dati relativi alle attività di competenza della unità organizzativa di assegnazione ai sensi dell'articolo 29 del GDPR e dell'articolo 2-*quaterdecies* del Codice Privacy, le istruzioni cui attenersi nel trattare i dati di cui ARERA è Titolare.
In caso di dubbi sull'interpretazione è possibile rivolgersi al RPD.

1. AMBITO DI APPLICAZIONE DEL GDPR

Sono soggetti alle prescrizioni del GDPR tutti i soggetti stabiliti nell'Unione europea e i soggetti che, ancorché non stabiliti, offrono beni o servizi, anche gratuitamente, a soggetti che si trovano nell'Unione, siano essi cittadini o meno di uno degli Stati membri.
Il GDPR non si applica esclusivamente ai trattamenti di dati personali effettuati da persone fisiche nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale, quali la corrispondenza e gli indirizzari, o l'uso dei *social network* e attività *online* intraprese nel quadro di tali attività.

2. COME TRATTARE I DATI

Nel trattare i dati personali di cui ai procedimenti e alle attività dell'unità organizzativa di assegnazione, ogni dipendente deve applicare i seguenti principi generali di cui all'articolo 5 del GDPR:

- liceità (rispetto delle norme), correttezza (rispetto delle reciproche esigenze dell'interessato e del titolare) e trasparenza (verso l'interessato affinché possa legittimamente fondare il proprio consenso) del trattamento dei dati personali;
- integrità e riservatezza: i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione;
- minimizzazione: i dati personali raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esattezza: i dati personali raccolti devono essere esatti e, se necessario, aggiornati anche prevedendo misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- limitazione delle finalità: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità o con il legittimo interesse del titolare;
- limitazione della conservazione: i dati personali devono essere 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 (i dati personali possono essere

conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici).

3. MISURE DI SICUREZZA ADEGUATE AL TRATTAMENTO

ARERA definisce le misure di sicurezza adeguate alle tipologie di trattamenti posti in essere. In generale, si ricorda che è fatto divieto di:

a) comunicare dati personali trattati per ragione di servizio a dipendenti di ARERA non appartenenti alla medesima unità organizzativa;
b) comunicare dati personali trattati per ragione di servizio a soggetti terzi che non siano stati preventivamente autorizzati 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.

3.1. Misure di sicurezza in caso di trattamenti cartacei

ARERA mette a disposizione dei dipendenti strumenti informativi volti a ridurre al minimo i trattamenti dei dati personali con modalità cartacee. Qualora il dipendente realizzi una copia analogica di un documento contenente dati personali deve:

a) custodirla in modo da evitare che terzi possano accedervi, ad esempio non lasciandola incustodita sulla scrivania o gettandola nei rifiuti;
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, utilizzando gli appositi distruggi documenti posizionati in ogni piano.

3.2. Misure di sicurezza in caso di trattamenti elettronici

Nell'ambito dei trattamenti operati tramite i sistemi informativi, ogni dipendente è tenuto a:

a) utilizzare esclusivamente i sistemi informativi, nonché i terminali e i *software* messi a disposizione da ARERA o da questa approvati, senza modificarne le impostazioni di sicurezza;
b) impedire che gli strumenti di lavoro o i supporti di memorizzazione (es. chiavette USB) forniti in dotazione da ARERA vengano utilizzati da terzi (es. familiari), in particolare se tali strumenti conservano dati personali;
c) custodire con cura e diligenza le credenziali per l'accesso e l'utilizzo dei sistemi informativi;
d) non cedere o divulgare le credenziali per l'accesso e l'utilizzo dei sistemi informativi a colleghi o terze persone;
e) non utilizzare sistemi di memorizzazione automatica delle credenziali di accesso nell'ipotesi in cui utilizzi un terminale di 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) nella trasmissione elettronica di dati personali (e-mail, servizi web, trasferimento file, instant messaging, ecc.) prestare sempre attenzione a individuare correttamente tutti i destinatari della trasmissione;
h) nella trasmissione di un messaggio di posta elettronica contenente dati personali:

1. valutare l'effettiva necessità di tale invio, verificare in particolare se il destinatario ha bisogno di ricevere tutti i dati o è sufficiente un sottoinsieme opportunamente scevro dei dati personali (a tal fine si consideri anche la possibilità che i dati siano già disponibili su altre applicazioni quali il protocollo informatico);
2. inviare il messaggio esclusivamente alle persone incaricate di quello specifico trattamento (prestare particolare attenzione agli indirizzi di gruppo e agli omonimi, specialmente quando il sistema di posta propone in automatico più indirizzi);
3. valutare se sia opportuno inviare un messaggio in modalità tale da non rendere visibili fra di loro i destinatari del messaggio;

i) nella ricezione di un messaggio di posta elettronica contenente dati personali:
   1. valutare che le informazioni afferiscano ad un trattamento specifico per il quale si è incaricati e che non siano informazioni già disponibili su altra applicazione, provvedendo in tal caso ad eliminare il messaggio ricevuto (dandone avviso al mittente con l'invito ad evitare il ripetersi della circostanza);
   2. valutare che le informazioni ricevute siano adeguate, pertinenti e limitate (minimizzazione dei dati) e, qualora così non fosse, eliminare, per quanto possibile, i dati in eccesso, eventualmente chiedendo al mittente un nuovo invio della documentazione limitata ai dati necessari (cancellando al contempo la documentazione ricevuta in precedenza);
   3. evitare di inoltrare le informazioni personali contenute nel messaggio se non strettamente richiesto dal trattamento in corso;
j) nell'utilizzo del protocollo informatico si applicano le stesse regole previste per l'invio e la ricezione di messaggi di posta elettronica, che valgono anche per la documentazione cartacea, ove presente;
k) nell'utilizzo dei sistemi di messaggistica istantanea (es. Microsoft Teams) si applicano le stesse regole previste per l'invio e la ricezione di messaggi di posta elettronica;
l) qualora si dovesse ricevere documentazione (di qualsiasi natura o formato) non sollecitata e/o non necessaria per i trattamenti in corso, provvedere immediatamente alla sua distruzione ove ciò sia tecnicamente possibile senza perdere l'informazione necessaria per l'attività istituzionale tenendo traccia dell'operazione, dandone comunicazione all'interessato se non già avvisato nella fase di richiesta;
m) non realizzare copie o *backup* dei dati su supporti removibili o terminali di proprietà;
n) controllare periodicamente le proprie cartelle di lavoro in locale e cancellare i file contenenti dati personali non più necessari ed aggiornare, se del caso, quelli utilizzati;
o) evitare di avere più copie di uno stesso file in cartelle diverse (es. su PC locale e su cartella di rete) per evitarne la proliferazione ed il conseguente rischio di perdita del controllo;
p) qualora si dovesse trovare, all'interno di una cartella di rete uno o più file contenenti dati personali condivisi con soggetti non autorizzati, segnalare quanto accaduto al Designato di secondo livello di riferimento;
q) evitare l'utilizzo di connessioni pubbliche non protette (es. reti di locali pubblici quali alberghi e ristoranti) o reti di Internet Point, preferendo l'utilizzo della sim dati messa a disposizione da ARERA, presente in tutti i dispositivi.

4. VIOLAZIONI DEI DATI PERSONALI (C.D. *DATA BREACH*)

Per «violazione dei dati personali» si intende, ai sensi dell'articolo 4 GDPR, ogni violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la

modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Alcuni possibili esempi di *data breach* sono:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Ogni dipendente, qualora venga a conoscenza o determini una potenziale violazione di dati, ne informa via mail, immediatamente, il Designato di primo e di secondo livello di riferimento, il RPD, e, se la sospetta violazione coinvolge sistemi informatici, il Responsabile SIN fornendo ogni elemento utile all'analisi degli accadimenti. La segnalazione può essere effettuata compilando e inviando il modulo A dell'Allegato 5 o fornendo le informazioni ivi richieste (data presunta di avvenuta violazione, data e ora in cui si è avuta conoscenza della presunta violazione, fonte della segnalazione, tipologia della violazione, descrizione evento anomalo, presunto numero di interessati coinvolti, quantità e caratteristiche dei dati personali interessati dalla presunta violazione, luogo in cui è avvenuta la violazione dei dati, eventuale descrizione dei *device* e dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione).

5. OBBLIGO DI FORMAZIONE E AGGIORNAMENTO

Ogni dipendente è tenuto a studiare il materiale informativo messo a disposizione da ARERA, anche tramite la sezione dedicata presente sul sito *intranet*, nonché a partecipare alle attività di studio e approfondimento, anche *online*, promosse dalla stessa.