ALLEGATO n. 2

Autorizzazione al trattamento dei dati personali

Al personale dell'Area …

Oggetto: Autorizzazione al trattamento dei dati personali da parte del Titolare del trattamento (art. 29 del GDPR n. 2016/679)

ATERSIR nella sua qualità di Titolare del trattamento dei dati personali (di seguito anche solo Titolare), rappresentato stante la designazione, quale soggetto delegato attuatore, dal sottoscritto Dirigente nome e cognome (indicare nome e carica per ognuno dei soggetti designati come da Deliberazione CAmb 97/2022)

designa

tutti i dipendenti dell'Area XXX quali incaricati del trattamento (di seguito Incaricato) di tutti i dati personali necessari allo svolgimento delle mansioni a ciascuno attribuite e svolte nell'ambito delle funzioni proprie dell'Area XXX.

Nell'espletamento delle mansioni a ciascuno assegnate e, in particolare, nell'effettuare le relative operazioni di trattamento di dati personali, ogni dipendente deve adeguare il proprio operato alle seguenti istruzioni, fornite ai sensi e per gli effetti dell'art. 29 del Regolamento.

1. Finalità, correttezza, liceità e trasparenza dei trattamenti di dati personali

1.1 Ogni dipendente ATERSIR, tratta i dati personali ai soli fini dello svolgimento della prestazione lavorativa richiesta e in stretta aderenza alle policy e alle istruzioni in materia di protezione dei dati personali e sicurezza informatica adottate dal Titolare del trattamento e, per questi, dai soggetti delegati attuatori.

1.2 Nessuno può, pertanto, trasferire i dati personali trattati a soggetti terzi, se non nei limiti e nel rispetto delle condizioni di liceità assolte dal Titolare del trattamento. Specificatamente, si

rappresenta che le operazioni di comunicazioni e/o diffusione di dati personali sono lecite se previste da norma di legge o regolamento.

1.3 Il Titolare fa sì che i trattamenti di dati personali degli interessati siano ispirati ai principi di correttezza, liceità, e trasparenza, fornendo agli stessi strumenti di trattamento adeguati. Inoltre, i dati personali che ciascun dipendente è autorizzato a trattare dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. In tutti i casi in cui ciascun dipendente ravvisi la sussistenza di dati eccedenti la finalità perseguita è tenuta ad avvisare il Responsabile della struttura a ciascun dipendente afferente.

1.4 Ciascun dipendente tratta i dati sottoposti a pseudonimizzazione da parte del Titolare con le medesime cautele e accorgimenti previsti per i dati personali.

1.5 Ciascun dipendente deve prestare particolare attenzione ed attenersi precipuamente alle istruzioni ricevute quando effettua trattamenti di dati personali suscettibili di cagionare danni, ovverosia nei casi in cui il trattamento comporta rischi di discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione; se sono trattati dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

1.6 Ciascun dipendente è tenuto, anche ai fini dell'eventuale valutazione d'impatto, a fornire al Titolare tutte le informazioni allo stesso utili per determinare il rischio del trattamento effettuato nell'esercizio delle mansioni assegnate.

2. Istanze da parte degli interessati e delle Autorità

2.1. Ciascun dipendente modifica o cancella i dati personali trattati nell'espletamento delle mansioni assegnate solo su specifica istruzione e autorizzazione del Titolare. Non sono ammesse operazioni di cancellazione e distruzione dei dati autonomamente determinate.

2.2. Nel caso di istanze effettuate, anche solo verbalmente, dagli interessati, ciascun dipendente deve avvisare immediatamente il Responsabile della struttura di ciascun dipendente afferenza e fornire allo stesso tutte le informazioni che consentano al Titolare di adempiere prontamente alle prescrizioni di legge.

2.3 Ciascun dipendente non dovrà richiedere o rintracciare ulteriori dati rispetto a quelli che il Titolare mette a disposizione e che non consentono l'identificazione di una persona fisica. Tuttavia, ciascun dipendente non rifiuta le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti.

2.4 Ciascun dipendente agevola, per quanto di sua competenza, il Titolare nell'evasione delle richieste promananti delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati.

3. Disposizioni per la sicurezza dei dati

3.1 Disposizioni per l'utilizzo delle risorse informatiche aziendali

In tutti i casi in cui utilizza la rete del Titolare, ciascun dipendente deve attenersi alle seguenti disposizioni:

- la configurazione di rete sulla propria postazione di lavoro può essere modificata solo dall'Amministratore di sistema a fronte di una formale autorizzazione da inoltrare al servizio tecnico il quale, preso atto delle motivazioni della richiesta, si farà carico di dare seguito alla richiesta secondo un ordine di priorità calcolato sulla base del livello di criticità e delle altre attività contingenti;
- l'accesso alla risorsa informatica è personale e vi si accede tramite nome utente e password di identificazione. L'accesso non può essere condiviso o ceduto tranne per casi specifici autorizzati per iscritto dal Titolare o suo delegato;
- gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi, compresi quelli di posta elettronica non dell'Ente, non espressamente e preventivamente autorizzati dall'Ente;
- la password è personale e non cedibile o trasmissibile a terzi fatta salva autorizzazione scritta da parte del Titolare o suo delegato: è fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, login e comunque chiavi di accesso riservate. Se smarrite va fatta immediatamente segnalazione e richiesta di sostituzione;
- l'utente, una volta ricevuto in uso un Computer o altro dispositivo, è tenuto a non alterare, né aggiungere e né cancellare, i software ivi installati;

- solo l'amministratore di sistema o il responsabile tecnico autorizzato provvede alla regolarizzazione delle licenze necessarie per il software presente sui computer del Titolare;
- è vietato distribuire e utilizzare fuori dal perimetro delle licenze acquistate di software soggetto a copyright;
- è vietato distribuire software che possano danneggiare le risorse informatiche, anche via e-mail;
- è vietato accedere fare copie di dati e/o programmi;
- solo l'amministratore di sistema o il responsabile tecnico autorizzato potrà accedere alla risorsa informatica dell'utente per compiti di aggiornamenti, ai fini della sicurezza del sistema e della rete;
- gli utenti sono obbligati a segnalare immediatamente ogni incidente, abuso o violazione della sicurezza, inviandone nota all'amministratore di sistema e/o al Responsabile della struttura di afferenza;
- gli utenti sono tenuti a partecipare alle iniziative di formazione organizzate dal Titolare e di esaminare le policy emanate dal Titolare o suo delegato in materia di privacy e sicurezza informatica;
- le postazioni di lavoro portatili, la carta e i supporti informatici, quando non presidiati per periodi di tempo significativi, devono essere sistemati in armadi adeguatamente chiusi o in altri contenitori fisicamente protetti.
- per tutto quanto non indicato alla presente si rimanda alle policy e procedure interne in materia di privacy e sicurezza dei dati.
- per quanto non specificato è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede.

3.2 Divieti relativi all'utilizzo di risorse informatiche assegnate

Si sottolinea inoltre che le risorse informatiche assegnate possono essere esclusivamente utilizzate per le attività istituzionali: non è assolutamente consentito l'uso per fini personali.

In particolare, e al solo fine di memoria, si ricorda che sono tassativamente vietate le seguenti attività:

- accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- diffondere prodotti informativi lesivi dell'onorabilità, individuali e collettivi;

- diffondere prodotti informativi di natura politica al di fuori di quelli consentiti dalla legge e dai regolamenti;
- diffondere, in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
- compiere attività che compromettono in qualsiasi modo la sicurezza delle risorse informatiche e della rete del Titolare;
- compiere attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, CD audio e video, clonazione o programmazione di smart card;
- utilizzare a titolo personale la posta elettronica assegnata;
- utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse informatiche (ad es. cracker, programmi di condivisione quali IRC, ICQ);
- intraprendere azioni allo scopo di:
  - degradare le risorse del sistema;
  - ottenere risorse superiori a quelle già allocate ed autorizzate;
  - accedere a risorse informatiche, sia dell'Ente che di terze parti, violandone le misure di sicurezza;
  - svelare le password altrui, nonché trasmettere in chiaro, pubblicare o mandare in stampa liste di account utenti o nomi host e corrispondenti indirizzi IP delle macchine;
- impedire ad utenti autorizzati l'accesso alle risorse;
- utilizzare software di monitoraggio della rete in genere;
- intercettare pacchetti sulla rete, utilizzare sniffer o software di analisi del traffico (spyware) dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali, del dipendente;
- utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente;
- accedere ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi;
- installare hub per sottoreti di PC e stampanti;
- installare modem per chiamate su linee analogiche, digitali o xDSL;
- installare modem configurati in call-back;
- accedere ai file di configurazione del sistema, farne delle copie e trasmetterle ad altri.

3.3 Disposizioni aggiuntive per gli assegnatari di dispositivi portatili

Nel caso Le sia reso disponibile l'uso di un personal computer portatile, di un tablet, o di altro dispositivo elettronico portatile, oltre a quanto previsto nei paragrafi precedenti, deve attenere il Suo operato alle seguenti ulteriori disposizioni:

- il dispositivo deve essere utilizzato esclusivamente da ciascun dipendente e solo ai fini strettamente connessi alle attività dell'Ente;
- il dispositivo non deve mai essere lasciato incustodito e comunque deve essere conservato di modo da minimizzare i rischi di furto, distruzione o manomissione;
- periodicamente il dispositivo deve essere riconsegnato al Titolare o ad apposito delegato, ai fini della verifica della sussistenza di aggiornamenti e patch non ancora installate.

Si richiama in particolare il modello organizzativo privacy (Delibera CAMB/2022/97 del 17 ottobre 2022) nonché le policy adottate dal Titolare in materia di privacy e sicurezza informatica (la cosiddetta "Data Breach") che, quindi, sono da intendersi parte integrante della presente autorizzazione, alle quali ciascun dipendente deve conformare il proprio operato.