Istruzioni operative per soggetto autorizzato al trattamento dei dati personali

In ottemperanza alle disposizioni del Regolamento UE 679/2016 per la protezione dei dati personali (GDPR 679/2016) e al Decreto Legislativo 196/2003 e smi (da ultimo con D.Lgs 101/2018), nello svolgimento delle operazioni di trattamento dei dati personali ogni soggetto dovrà attenersi con scrupolo e diligenza alle seguenti istruzioni e ad ogni ulteriore indicazione, scritta e/o verbale, che potrà essere fornita dal Delegato o dal Titolare stesso.

☐ **Trattamento di dati personali**

L'Art. 4 del GDPR 679/2016 definisce il trattamento di dati personali come *"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."*

Il trattamento dev'essere:

a) effettuato secondo modalità tali da garantire la riservatezza;
b) effettuato in modo lecito e corretto e trasparente nei confronti dell'interessato;
c) raccolti per finalità determinate, esplicite e legittime;
d) realizzato in modo che non sia incompatibile con tali finalità;
e) limitato a quanto necessario rispetto alle finalità per le quali è stato raccolto;
f) deve avvenire in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale;
g) trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.

☐ **Obblighi formali**

Ogni soggetto autorizzato al trattamento dati è tenuto a:

- attuare le misure necessarie per un corretto, lecito, sicuro trattamento, attenendosi alle istruzioni operative;
- tenere aggiornato l'elenco dei trattamenti a Lei affidati con le indicazioni relative alla tipologia dei dati trattati, alle banche dati, agli strumenti elettronici, all'ubicazione di detti strumenti e degli archivi informatici e cartacei;
- utilizzare le banche dati informatiche esclusivamente attraverso le proprie credenziali di autenticazione da tenere riservate, richiedere l'autorizzazione al proprio Delegato Privacy per le modifiche e/o integrazioni del profilo autorizzativo che si rendessero necessarie;
- disporre quanto necessario a garantire la sicurezza dei locali di trattamento ed archiviazione dei dati, adottando idonee misure contro accessi non autorizzati;
- ottemperare agli obblighi di informazione e acquisizione del consenso, quando non altrimenti eseguito dalla struttura nei confronti degli interessati;
- controllare e custodire, durante il compimento dell'intero trattamento e fino alla consegna, gli atti e i documenti contenenti dati, personali sensibili o giudiziari, in modo da impedirne l'accesso a persone non autorizzate;
- informare il proprio Delegato Privacy in merito alle eventuali richieste dell'interessato di esercitare i diritti previsti dagli artt. 12, 13 e 14 del GDRP 679/2016.

☐ **Accesso banche dati e Divieto di duplicazione banche dati**

L'accesso alle banche dati è limitato agli utilizzi previsti dalle mansioni attribuite al soggetto autorizzato. Non sono ammesse duplicazioni di data base contenenti dati personali, se non previa autorizzazione del Responsabile o Titolare.

☐ **Utilizzo e trasmissione dei dati**

I dati oggetto di trattamento non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative. Nessun dato personale può essere utilizzato o trasmesso all'esterno senza previa autorizzazione del Responsabile o del Titolare.

☐ **Strumenti informatici**

Al fine di garantire un corretto trattamento dei dati nel rispetto delle misure di sicurezza che l'azienda ha ritenuto idoneo adottare, è opportuno impiegare gli strumenti elettronici ed informatici con diligenza ed attenzione, attenendosi alle disposizioni contenute nel *"Regolamento per l'utilizzo dei Sistemi Informativi Aziendali"*, reso disponibile all'atto dell'assunzione e consultabile nell'Intranet aziendale.

A compendio di quanto indicato nel suddetto regolamento, sono comunque impartite queste direttive:

- Il trattamento di dati personali con strumenti elettronici è consentito alle figure dotate di credenziali di autenticazione (password riservata) che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti;
- I criteri di impostazione delle credenziali di autenticazione, così come la tempistica di cambiamento delle stesse, vengono comunicate dal Titolare del trattamento e/o di un suo delegato in relazione alla natura dei dati trattati e ai rischi sottesi a tali trattamenti;
- Non è consentito comunicare a nessuno le proprie password e soprattutto le stesse non vanno scritte su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;
- Non è consentito lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Non è consentito installare sulla propria postazione di lavoro programmi non attinenti alle normali attività d'ufficio né nuovi programmi necessari senza la preventiva autorizzazione del Titolare del trattamento e/o del suo delegato;
- Non è consentito modificare le configurazioni hardware e software senza 'autorizzazione del Titolare del trattamento e/o del suo delegato;
- Se si rileva un problema nell'ambito dell'utilizzo del sistema informatico relativo al trattamento di dati in corso che può compromettere la sicurezza dei dati se ne dà immediata comunicazione al Responsabile della U.O.S.D. Sistemi Informativi;
- Accertarsi che sul proprio computer sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva;
- Sottoporre a controllo con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna prima di eseguire files in essi contenuti;
- Accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;
- Non è consentito scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti;
- Utilizzare la connessione ad Internet esclusivamente per lo svolgimento dei propri compiti istituzionali;
- Segnalare qualsiasi anomalia o stranezza di comportamento al Titolare del trattamento e/o ad un suo delegato.

☐ **Credenziali**

Per il trattamento dei dati con gli strumenti elettronici in dotazione alla struttura il soggetto autorizzato viene dotato di credenziali di accesso (*username* e *password*).

Tali credenziali sono strettamente personali ed identificano l'operatore nella rete informatica.

-Le caratteristiche e le norme da applicarsi a tutte le credenziali in uso al soggetto autorizzato, sono definite nel *"Regolamento per l'utilizzo dei Sistemi Informativi Aziendali"*, reso disponibile all'atto dell'assunzione e consultabile nell'Intranet aziendale.

☐ **Documenti cartacei**

I dati presenti su documenti cartacei devono essere tutelati mediante conservazione e gestione degli stessi in modo da evitarne la visibilità, la sottrazione, la riproduzione, l'alterazione o distruzione abusiva.

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (*es. armadi o cassetti chiusi a chiave, uffici chiusi a chiave*).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie stampanti, fotocopiatrici, fax o tavoli di lavoro.
- I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che

non ne necessitano per lo svolgimento delle proprie mansioni lavorative (*anche se queste persone sono a loro volta soggetti autorizzati del trattamento*).

- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili;
- I documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli incaricati, i quali devono impedire l'accesso a persone prive di autorizzazione;
- L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

☐ **Rilascio Credenziali**

Unitamente alla presente le vengono rilasciate le seguenti credenziali di accesso (*) ai sistemi e servizi aziendali:

- Utente di dominio: _____
- Casella di posta elettronica: _____
- Utente di procedure: per il rilascio delle credenziali devono essere utilizzati gli appositi moduli .

(*) La parte privata delle credenziali di accesso (password) viene rilasciata con altro documento disgiunto.

☐ **Presa visione**

Il soggetto firmatario conferma di aver preso visione sia delle istruzioni operative dettagliate nei paragrafi precedenti, che dei regolamenti citati nei vari paragrafi.

Data_____ Firma _____

(soggetto destinatario della presente istruzione)