

**STRUTTURA:** .....

Il Preposto al trattamento .....

**DESIGNA**

Il/la dipendente .....

I dipendenti: .....

.....

.....

I dipendenti con profili di: .....

**INCARICATO DEL TRATTAMENTO  
INCARICATI DEL TRATTAMENTO**

relativamente alle operazioni effettuate nello svolgimento dei compiti assegnati nell'ambito delle attività di competenza.

L'incaricato del trattamento non può trattare dati se non sono individuate le operazioni di trattamento autorizzate e non riceve istruzioni dal Titolare o dal Preposto sulle corrette modalità della loro effettuazione.

**BANCHE DATI E OPERAZIONI DI TRATTAMENTO AUTORIZZATE**

Le banche dati alle quali, nell'ambito della prestazione lavorativa, si autorizza l'accesso sono le seguenti: *(elencare banche dati/sistemi applicativi)*

.....

.....

.....

In relazione ai dati presenti nelle suddette banche dati, sono autorizzate le operazioni di trattamento sottoelencate, osservando le istruzioni del Titolare/Preposto *(spuntare le operazioni autorizzate)*:

- raccolta e registrazione
- consultazione
- estrazione
- comunicazione
- elaborazione
- modificazione
- utilizzo
- interconnessione
- cancellazione

## PRINCIPI DI CARATTERE GENERALE

L'incaricato del trattamento deve:

- rispettare le prescrizioni della vigente normativa in materia di protezione dei dati personali, secondo le istruzioni impartite in ambito aziendale e, in particolare, dal proprio Preposto al trattamento;
- effettuare operazioni di trattamento di dati personali soltanto per le finalità e con le modalità strettamente correlate allo svolgimento delle attività di competenza, con divieto di qualsiasi altra diversa utilizzazione;
- accedere ai soli dati personali, comprese le categorie particolari di dati di cui all'art. 9 del RGPD<sup>1</sup> e i dati relativi a condanne penali e reati di cui all'art. 10 del RGPD strettamente necessari allo svolgimento delle funzioni assegnate;
- trattare i dati personali di cui si venga a conoscenza nell'ambito dello svolgimento delle proprie funzioni in modo tale da garantire, in ogni operazione di trattamento, la massima riservatezza, osservando tali doveri di riserbo anche dopo la cessazione dalla attività di servizio;
- verificare che i dati acquisiti dagli interessati o da soggetto terzi siano esatti e completi e siano utilizzati in modo pertinente e non eccedente rispetto alle attività svolte e ai compiti assegnati;
- comunicare dati (cioè metterli a disposizione di soggetti esterni preventivamente determinati) solo dopo aver accertato la liceità e legittimità dell'operazione, anche in riferimento alle modalità con cui si intende effettuarla;
- effettuare il trasferimento di dati ad altre strutture interne all'Azienda (tale operazione non è tecnicamente riconducibile ad una *comunicazione* di dati), tenendo presente che è comunque consentita nei limiti delle finalità istituzionali perseguite dalla struttura o dai soggetti destinatari e sempre in base ad un principio di necessità, pertinenza e non eccedenza (si qualifica negli stessi termini la trasmissione di dati nell'ambito di un rapporto contrattuale/convenzionale instaurato dall'Azienda con terzi per l'esternalizzazione di attività/funzioni/servizi, a condizione che il terzo sia stato nominato Responsabile del trattamento dei dati ai sensi dell'art. 28 del RGPD);
- diffondere dati (metterli cioè a disposizione di soggetti indeterminati) solo dopo aver accertato la liceità e legittimità dell'operazione, anche in riferimento alle modalità con cui si intende effettuarla, fatto salvo l'assoluto divieto di diffondere dati idonei a rivelare lo stato di salute.
- non effettuare, alla cessazione dell'attività di dipendenza/collaborazione con l'Azienda, operazioni di trattamento dei dati personali di sia cui venuto in possesso o a conoscenza durante lo svolgimento dell'incarico e, in particolare, non conservarli, duplicarli, comunicarli o cederli ad altri.

<sup>1</sup> Il RGPD definisce tali i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

## **OBBLIGHI DI CARATTERE INFORMATIVO**

L'incaricato del trattamento deve:

- informare tempestivamente il Preposto e, se necessario, il Responsabile della protezione dei dati, di ogni questione rilevante in relazione al trattamento di dati personali effettuato e di eventuali richieste da parte dei soggetti cui i dati si riferiscono;
- qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni di sicurezza dei dati personali che possano esporre a rischio di violazione dei dati (data breach), informare immediatamente il Preposto al trattamento;
- segnalare al Preposto al trattamento eventuali circostanze che richiedano il necessario ed opportuno aggiornamento delle misure di sicurezza, tecniche come organizzative, adottate, al fine di ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità del medesimo;

## **OBBLIGHI CIRCA L'USO DELLA POSTAZIONE DI LAVORO INFORMATICA E DELLA RETE AZIENDALE**

L'incaricato del trattamento deve:

- adottare, in caso di allontanamento dalla propria postazione di lavoro, tutte le cautele necessarie ad evitare l'accesso ai dati personali trattati o in trattamento da parte di terzi, anche se dipendenti;
- evitare, in particolare, di lasciare la propria stazione di lavoro incustodita e collegata con il proprio account all'ambiente di rete, chiudendola o bloccandola in tutte le occasioni in cui si assenti dall'ufficio;
- utilizzare, per l'accesso alle banche dati automatizzate, il proprio codice personale, al fine di consentire sempre l'individuazione di chi ha effettuato una operazione di trattamento;
- non utilizzare la rete aziendale per fini non espressamente autorizzati e tenere un comportamento corretto durante la navigazione in internet;
- valutare, prima di trasmettere via e-mail dati personali ed in particolari riconducibili alle categorie di dati di cui agli artt. 9 e 10 del RGPD, la liceità e la legittimità dell'operazione, nonché le modalità di essa (in particolare, si raccomanda il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero il ricorso all'uso di codificazione dei dati contenuti nel testo delle comunicazioni);
- evitare di alterare la configurazione software della stazione di lavoro.

---

## **OBBLIGHI CIRCA L'UTILIZZO DELLE PASSWORD**

L'incaricato del trattamento deve:

- mantenere riservate e nella sua esclusiva disponibilità le credenziali d'autenticazione, ovvero username/password o smart card/password (in caso di prolungata assenza o impedimento dell'incaricato, al titolare è comunque assicurata, qualora sia indispensabile e indifferibile, per esclusive necessità di operatività e di sicurezza del sistema, la disponibilità dei suddetti dati e strumenti).

In particolare, la password deve essere attivata ed utilizzata secondo le seguenti modalità:

- deve essere costituita da almeno 8 caratteri o comunque deve avere la lunghezza massima consentita dal sistema, utilizzando un misto di lettere, numeri e segni di interpunzione;
- non deve essere costituita utilizzando segni che possano essere facilmente riconducibili all'identità dell'utente (ad esempio, il codice fiscale, il nome del coniuge o dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della via ove si abita, il proprio numero di matricola o addirittura lo stesso user name, ecc), o ottenute da una combinazione di tasti vicini alla tastiera o sequenze di caratteri;
- è modificata (dall'incaricato, anche se la modifica non è proposta dal sistema) almeno ogni tre mesi in caso di trattamento delle categorie di dati di cui agli artt. 9 e 10 del RGPD, e ogni sei mesi negli altri casi;
- non deve essere comunicata a nessuno, e non deve essere trascritta su supporti facilmente rintracciabili, in particolare in prossimità della postazione di lavoro;
- digitata accertandosi che non ci sia nessuno che osservi e sia in grado di vedere o intuire i caratteri digitati sulla tastiera.

## **OBBLIGHI PER LA GESTIONE DELLA DOCUMENTAZIONE CARTACEA**

L'incaricato del trattamento deve:

- garantire la corretta custodia e la riservatezza dei documenti cartacei utilizzati per le attività di competenza, non lasciando incustodita o esposta alla visione di soggetti comunque non legittimati (compresi altri incaricati non abilitati al trattamento) la documentazione cartacea, ed in particolare controllare e custodire fino alla restituzione gli atti e i documenti contenenti le categorie di dati di cui agli artt. 9 e 10 del RGPD;
- in particolare, riporre i documenti che contengono le categorie di dati di cui agli artt. 9 e 10 del RGPD in archivi ad accesso controllato (armadi/schedari/contenitori muniti di serratura oppure soggetti a sorveglianza da parte di personale a ciò deputato);
- controllare che ogni dispositivo idoneo a stampare documenti sia disposto in modo che la visione dei documenti in uscita sia possibile solo da parte del personale incaricato al trattamento dei dati, attivando in caso contrario il Preposto al trattamento e, in caso di utilizzo di stampanti, fotocopiatrici o fax condivisi da

- vari utenti e collocati al di fuori dei locali ove è posta la singola stazione di lavoro, raccogliere immediatamente le stampe e custodirle con le modalità sopra descritte;
- effettuare il trasferimento di ogni documento contenente le categorie particolari di dati di cui agli artt. 9 e 10 del RGPD adottando rigorose misure di garanzia, tali da impedire che allo stesso accedano estranei: buste chiuse, documenti sigillati, non abbandono durante i trasferimenti;
  - sincerarsi che al momento dello spegnimento dei PC non vi siano documenti in coda di stampa;
  - non riprodurre o fotocopiare documenti se non per esigenze connesse alla finalità del trattamento;
  - distruggere eventuali fotocopie o stampe mal riuscite di documenti contenenti dati personali;
  - qualora proceda all'acquisizione in formato digitale della documentazione cartacea a mezzo scanner, verificare che l'operazione sia avvenuta correttamente e che il documento oggetto di scansione sia correttamente rimosso ed archiviato dopo l'effettuazione dell'operazione;
  - qualora riceva nel proprio ufficio utenti e cittadini e tenga sulla propria scrivania cartelle e fascicoli, rimuovere le stesse o evitare di inserire (a seconda delle necessità operative e organizzative) sul frontespizio delle stesse dati ed informazioni che permettano a terzi estranei di percepire l'identità dei soggetti interessati dal trattamento.

### **OBBLIGHI PER IL RISPETTO DEI DIRITTI DEGLI INTERESSATI**

L'incaricato del trattamento deve:

- verificare che gli utenti siano portati a conoscenza dell'informativa sul trattamento dei dati personali ed acquisire dagli stessi, laddove previsto, il consenso al trattamento;
- assicurare che gli ordini di precedenza e di chiamata per prestazioni sanitarie prescindano dalla individuazione nominativa degli interessati;
- in caso di richiesta o di fruizione di prestazioni sanitarie e/o amministrative, porre in essere tutte le misure individuate dal Preposto al trattamento finalizzate delimitare apposite distanze di cortesia o comunque atte a garantire la riservatezza degli utenti, in particolare in sala d'attesa e nei locali ove si svolgono i colloqui sanitari;
- non esporre al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati, né liste nominative di prestazioni ambulatoriali, di diagnostica strumentale e di laboratorio e di altre prestazioni sanitarie in genere;
- dare informazioni, anche per telefono, limitatamente alla presenza di una persona al pronto soccorso o in reparto (senza dare notizie sullo stato di salute) solo a terzi legittimati (parenti, familiari, conviventi, conoscenti, volontari), in ogni caso rispettando l'eventuale volontà contraria espressa dal paziente e raccolta al momento dell'accesso;
- rispettare le indicazioni espresse dal paziente negli appositi moduli aziendali circa i soggetti autorizzati a ricevere comunicazioni sul suo stato di salute;

- porre in essere soluzioni e misure atte a evitare che soggetti estranei possano collegare il paziente al suo stato di salute; ad es. nella spedizione di prodotti/referti/documentazione sanitaria o amministrativa correlata alla prestazione sanitaria, non riportare sulla parte esterna del plico postale informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato (quali ad es. indicazione della tipologia del contenuto del plico o del reparto/struttura dell'organismo sanitario mittente). Tali cautele devono essere adottate anche nelle eventuali certificazioni/attestazioni richieste per fini amministrativi non correlati a quelli di cura (ad. es per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi a una procedura concorsuale)
- consegnare referti/documentazione sanitaria di norma in busta chiusa, e qualora si presenti per il ritiro un soggetto diverso dall'interessato procedere alla consegna solo in presenza di delega scritta da parte dell'interessato e dei documenti di riconoscimento del delegato e dell'interessato;
- non utilizzare strumenti di social networking per la condivisione di dati personali riferiti a pazienti;
- non raccogliere immagini dei pazienti mediante dispositivi elettronici di ripresa non autorizzati, inclusi telefoni cellulari.

Luogo e data \_\_\_\_\_

IL PREPOSTO AL TRATTAMENTO DATI PERSONALI  
\_\_\_\_\_

L'INCARICATO \_\_\_\_\_

L'INCARICATO \_\_\_\_\_

*(L'originale del presente atto viene consegnato all'incaricato; una copia deve essere conservata agli atti presso la struttura)*

CONTATTI RESPONSABILE PROTEZIONE DATI

tel.0575 254156

e-mail: [privacy@uslsudest.toscana.it](mailto:privacy@uslsudest.toscana.it)

GLOSSARIO

**Dato personale** - 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.

**Categorie particolari di dati personali** - i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

**Trattamento** - 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.

**Interessato** - la persona fisica, identificata o identificabile, cui si riferiscono i dati personali trattati.

**Titolare del trattamento** - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

**Responsabile del trattamento** - la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

**Incaricati del trattamento** - le persone fisiche autorizzate dal Titolare al trattamento dei dati personali.

**Responsabile della protezione dei dati** - soggetto con il compito di sorvegliare ed implementare l'osservanza del RGPD.

**Registro delle attività di trattamento** - il registro delle attività di trattamento svolte sotto la responsabilità del titolare.

**Valutazione di Impatto sulla Protezione dei dati** - processo dovuto e formale - finalizzato ad analizzare e descrivere un trattamento di dati personali, valutarne necessità e proporzionalità, effettuare una valutazione dei rischi per i diritti e le libertà degli interessati, definire le misure tecniche e organizzative (comprese le misure di sicurezza adeguate) che il titolare ritiene di dover adottare allo scopo di mitigare tali rischi - da effettuarsi prima dell'inizio del trattamento, allorché questo "possa presentare un rischio elevato" per i diritti dell'interessato; per i trattamenti in corso, che possano presentare un rischio elevato per i diritti e le libertà degli interessati, da attivarsi qualora siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi.

**Violazione dei dati personali (data breach)** - la 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.