Azienda Sanitaria Locale della Provincia di Foggia

ISTRUZIONI GENERALI
SUL TRATTAMENTO DEI DATI PERSONALI
PER TUTTO IL PERSONALE AZIENDALE

INDICE

Premessa

Gentile Dipendente/Collaboratore,

l'ASL di Foggia, in qualità di Titolare del trattamento dei dati, La informa che ai sensi della vigente normativa in materia di protezione dei dati, **Lei è designato quale soggetto autorizzato al trattamento dei dati personali che il suo ruolo e funzione richiedono**.

Il soggetto autorizzato è la persona fisica che, nell'ambito delle proprie specifiche competenze professionali, sotto l'autorità diretta del Titolare, ed attenendosi alle istruzioni impartite dallo stesso o dal Delegato (Direttore/Responsabile), compie operazioni di trattamento dei dati personali e particolari (sensibili e giudiziari).

Di seguito il **Titolare del trattamento dei dati intende impartire una serie di istruzioni generali** necessarie per conformare il trattamento dei dati alla vigente disciplina in materia di protezione dei dati personali e per evitare comportamenti sanzionabili dall'Autorità Garante per la protezione dei dati personali.

Ciascun dipendente/collaboratore riceverà istruzioni specifiche sul trattamento dei dati dal Responsabile Dirigente della Struttura di assegnazione.

Introduzione

Il Regolamento Generale sulla Protezione dei Dati (Reg. UE/2016/679), in sigla GDPR (*General Data Protection Regulation*), la nuova normativa europea in ambito di protezione dei dati personali dei cittadini europei e di tutti coloro che si trovano sul territorio UE, uniforma la legislazione di tutti gli Stati membri dell'UE, con l'obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto al trattamento dei dati ed assicurare la libera circolazione dei dati personali tra Stati Membri. Inoltre, dal 19 settembre 2018, l'entrata in vigore del decreto legislativo n. 101/2018 di adeguamento del Codice in materia di protezione dei dati personali (D.lgs. 196/03), ha dato vita ad un quadro normativo di non facile interpretazione. Il nuovo Regolamento presenta un apparato sanzionatorio molto severo, con multe che possono arrivare fino a 20 milioni di euro o al 4% del fatturato globale del trasgressore. L'ambito sanitario risulta particolarmente critico in considerazione della tipologia dei dati trattati e della vulnerabilità dei soggetti interessati.

Alle persone che entrano in contatto con medici e strutture sanitarie per cure, prestazioni mediche ed operazioni amministrative, devono essere garantite la più assoluta riservatezza ed il rispetto della dignità. I dati personali in grado di rivelare lo stato di salute delle persone sono infatti di particolare delicatezza, per questo definiti "dati sensibili" o dati appartenenti a "categorie particolari" e non possono essere diffusi.

Ad essi il vigente Codice in materia di protezione dei dati personali (D.lgs 196/03, così come modificato dal D.lgs 101/18) attribuisce una tutela rafforzata e stabilisce le regole per il loro trattamento in ambito sanitario, tenendo sempre conto del ruolo professionale dei medici e del personale paramedico.

Principali definizioni

Ai fini delle presenti istruzioni s'intende per:

1) «**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;

2) «**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;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «**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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del

trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**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;

9) «**responsabile della protezione dei dati**»: è il soggetto designato dal Titolare (DPO o RPD) con il compito principale di sorvegliare l'osservanza del Regolamento generale sulla protezione dei dati;

10) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

11) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

12) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

13) «**violazione dei dati personali**»: 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;

14) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

15) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

16) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Principi generali del trattamento dei dati personali (art. 5 GDPR)

Tutti i dipendenti, nello svolgimento delle attività lavorative che comportano il trattamento di dati personali, devono attenersi ai seguenti principi:

-

- **Liceità, correttezza e trasparenza**
  – i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
- **Limitazione della finalità**
  – i dati devono essere raccolti e trattati esclusivamente per finalità determinate, esplicite e legittime, evitando usi successivi incompatibili con tali scopi.
- **Minimizzazione dei dati**
  – devono essere trattati solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità perseguite.
- **Esattezza**
  – i dati devono essere aggiornati ed esatti; quelli inesatti devono essere tempestivamente rettificati o cancellati.
- **Limitazione della conservazione**
  – i dati devono essere conservati per un periodo non superiore a quello necessario al conseguimento delle finalità del trattamento, nel rispetto dei piani di conservazione aziendali.
- **Integrità e riservatezza**
  – i dati devono essere trattati in modo da garantire adeguata sicurezza, inclusa la protezione contro trattamenti non autorizzati o illeciti, nonché da perdita, distruzione o danno accidentale.
- **Accountability (**responsabilizzazione)
  – l'Amministrazione e ciascun dipendente, per quanto di competenza, devono poter dimostrare il rispetto dei principi sopra indicati.

Istruzioni generali per il trattamento dei dati

Di seguito vengono riportate una serie di regole e di istruzioni, che devono essere osservate dal dipendente preposto allo svolgimento delle operazioni di trattamento per conto dell'ASL di Foggia:

a) istruzioni per lo svolgimento delle operazioni caratterizzanti il processo di trattamento:

- **raccolta:**

prima di procedere alla raccolta dei dati personali, ai sensi degli artt. 13-14 del Regolamento UE 2016/679, deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati secondo le disposizioni del Titolare; occorre procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza, la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento in conformità

a quanto previsto dalla legge e dai regolamenti, seguendo le istruzioni del Titolare e del Responsabile della Struttura di appartenenza (designato interno al trattamento dei dati);

- registrazione:

non lasciare fogli, cartelle e quant'altro a disposizione di estranei;

- **conservazione:**

i documenti o gli atti che contengono dati sensibili o giudiziari devono essere conservati in archivi ad accesso controllato. E' quindi necessario garantire che armadi, schedari e contenitori siano muniti di serratura o che il soggetto autorizzato al trattamento, che riceva utenti e assistiti, sia sempre presente nella propria stanza o luogo di lavoro avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. Sarà cura di ciascun Responsabile di Struttura adottare i provvedimenti necessari affinché venga escluso un accesso ad archivi e dati da parte di soggetti che non siano autorizzati al trattamento;

- **utilizzo:**

i dati possono essere utilizzati solo da coloro che sono stati espressamente autorizzati al trattamento dal proprio superiore gerarchico. L'utilizzo dei dati deve avvenire solo per scopi determinati, espressi e legittimi, avendo cura di evitare un utilizzo per scopi che non coincidano o che non siano compatibili con quelli istituzionali;

- **blocco:**

questa operazione può essere conseguenza di una espressa richiesta da parte dell'interessato ovvero può essere ordinata direttamente dal Garante per la protezione dei dati personali;

- **comunicazione di dati personali:**

per comunicazione si intende il "dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare, dal responsabile e dalle persone autorizzate al trattamento dei dati dal Titolare (dipendenti e collaboratori)". Qualora il richiedente i dati personali sia un soggetto pubblico, la comunicazione dei dati personali diversi da quelli sensibili potrà avvenire, pur in mancanza di espressa previsione di legge o di regolamento, qualora sia necessaria per l'esercizio di una delle finalità istituzionali dell'Ente destinatario della stessa comunicazione. In tal caso la comunicazione può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati;

- **diffusione:**

per diffusione si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

La pubblicazione di qualsiasi atto (in “albo pretorio”, in “amministrazione trasparente”, in una bacheca, su internet etc.) che contenga dati personali costituisce, ai sensi del vigente Codice in materia di protezione dei dati personali, una forma di diffusione di informazioni personali. La diffusione di dati personali è ammessa solo se prevista da una norma di legge o di regolamento.

Istruzioni per il corretto utilizzo degli strumenti informatici

Di seguito alcune importanti istruzioni per un corretto utilizzo della strumentazione informatica aziendale:

- **Computer:**

tutte le volte che si abbandona la propria postazione di lavoro si deve aver cura di porre il pc/terminale in condizione da rendere i dati non accessibili ad estranei non autorizzati. (potrebbe ad es. essere sospesa la propria sessione di lavoro disconnettendosi dall’applicazione in uso);

- **E-mail ed uso di Internet:**

la posta elettronica deve essere utilizzata per scopi di ufficio. Si ricorda che qualunque comunicazione ricevuta o spedita utilizzando l’indirizzo di posta aziendale non è corrispondenza personale dell’operatore, per cui potrebbero essere effettuati controlli remoti al fine di verificare l’uso improprio o illecito degli strumenti forniti in dotazione;

Occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica (ordinaria e certificata), di file o di messaggi contenenti dati sensibili (ad es. dati sanitari degli assistiti). In tal caso, occorrerà proteggere il contenuto del file dall’accesso e dalla visione di soggetti non autorizzati o non legittimati al trattamento diversi dai destinatari delle comunicazioni elettroniche considerate. A titolo meramente esemplificativo, si consiglia il ricorso all’uso di password per l’apertura dei documenti oppure tecniche di cifratura dei messaggi, ovvero all’utilizzo di codici identificativi (c.d. *pseudonimizzazione*) dell’identità dell’interessato associati ai dati sensibili e/o giudiziari, in modo da rendere non comprensibili i dati nel caso di intercettazione delle comunicazioni;

- **file di log:**

tutti gli accessi ai computer e ai sistemi gestionali aziendali sono tracciati attraverso un sistema di registrazione dei log, al fine di poter risalire all’esecutore di specifiche operazioni in caso di necessità. Pertanto risulta di fondamentale importanza accedere al computer tramite le proprie credenziali nominative senza mai condividere la propria password con altri colleghi;

-telefono:

è assolutamente necessario non fornire per mezzo del telefono dati ed informazioni di carattere sanitario o di natura comunque riservata qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione ad ottenere i dati richiesti del soggetto chiamante. Si consiglia, qualora si nutrano dubbi sull'identità di chi è dall'altra parte dell'apparecchio, di richiedere identità e qualità dell'interlocutore al fine di richiamarlo successivamente per avere certezza sulla identità;

- **supporti informatici** (cd-rom/dvd/chiavette usb/dischi esterni):

i supporti informatici già utilizzati per il trattamento di dati sensibili e giudiziari possono essere riutilizzati solo nel caso in cui le informazioni precedentemente contenute non siano più in alcun modo recuperabili, in caso contrario devono essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

- **spedizione di documenti a mezzo posta**:

la documentazione contenente dati sensibili o giudiziari deve essere trasmessa, anche all'interno dell'azienda ove possibile, in busta chiusa, in modo da assicurare la protezione della riservatezza sia del documento che dei dati contenuti;

- **uso di software**:

è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte del Responsabile dei Sistemi informativi aziendali. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito, sia di natura penale che civile, secondo quanto previsto dalla legge sul diritto d'autore, così come integrata dal D.Lgs. 518/1992 e successive modificazioni e integrazioni;

- **uso di WhatsApp**:

L'uso di WhatsApp presenta potenziali aspetti positivi in ambito sanitario fra cui la sensibilizzazione a tematiche di salute e prevenzione, il reclutamento di pazienti in programmi di ricerca e attività di raccolta di fondi. Tuttavia esiste la possibilità di disseminazione incontrollata di informazioni personali suscettibili di recare pregiudizio ai diritti e alle libertà degli interessati. Pertanto, al fine di evitare comportamenti in violazione della vigente normativa in materia di protezione dei dati, è vietato l'utilizzo di whatsapp e applicazioni analoghe (telegram etc.) per finalità di invio/ricezione di documentazione sanitaria o riservata, salvo differenti disposizioni del Titolare che definirà le misure di garanzia necessarie;

Misure di Sicurezza

c) **password:**

La credenziale di accesso ai Pc e ai Gestionali aziendali (nome utente e password) deve essere modificata obbligatoriamente al primo accesso (dopo aver ricevuto la prima password), composta da un minimo di otto caratteri e di tipo nominativa; deve essere modificata dal dipendente ogni 60 giorni con eventuali sistemi automatici centralizzati aziendali; non deve contenere riferimenti agevolmente riconducibili al dipendente e dovrebbe essere generata preferibilmente senza un significato compiuto. Nello scegliere la password, è necessario utilizzare anche caratteri speciali e lettere maiuscole e minuscole. La password di accesso ai computer e gestionali aziendali deve essere custodita con la massima attenzione e segretezza senza comunicarla a colleghi o soggetti esterni;

b) **Copie salvataggio dati:**

Salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere, con cadenza almeno settimanale, all'effettuazione di copie di sicurezza (backup) dei dati oggetto di trattamento, utilizzando gli strumenti aziendali disponibili. Riporre le copie di salvataggio in un contenitore al quale possano accedere solamente i soggetti autorizzati. E' vietato effettuare copie di salvataggio di dati aziendali su supporti di memoria di proprietà personale (penne usb, copia su dischi in cloud personale etc.);

c) **antivirus:**

I computer in rete sono provvisti di antivirus aziendale gestito centralmente tuttavia tutto il personale aziendale è tenuto a segnalare tempestivamente eventuali anomalie o sospetti problemi di sicurezza all'amministratore di sistema.

Per dettagli e aggiornamenti si rinvia al vigente Regolamento per l'utilizzo e gestione delle risorse strumentali informatiche e telematiche aziendali.

Segnalazione delle violazioni

L'art. 4 del Regolamento Europeo sulla protezione dei dati definisce la **violazione dei dati personali** (*c.d. data breach*) come "*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*".

Quindi, un *data breach* non è solo un evento **doloso** come un attacco informatico, ma può essere anche un evento **accidentale** come un accesso abusivo, un incidente (es. un incendio o allagamento), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un Pc, notebook o smartphone di un dipendente).

In caso di violazione dei dati personali il dipendente è tenuto a segnalare immediatamente l'evento al Responsabile della protezione dei dati e per quanto di competenza, al Responsabile dei Sistemi informativi aziendali, per i conseguenti adempimenti.

Per dettagli si rinvia alla vigente procedura per la gestione dei data breach.

Rapporti con l'utenza

- **identificazione dell'interessato:**

Al fine di garantire la corretta verifica dell'identità della persona che esercita diritti o presenta istanze, può rendersi necessario richiedere la copia di un documento di identità o di riconoscimento.
Tale documentazione sarà trattata esclusivamente per le finalità di identificazione, custodita in modo sicuro (ad es. in armadi chiudibili a chiave o sistemi informatici protetti) e conservata per il solo periodo strettamente necessario al perseguimento delle predette finalità, in conformità al piano di conservazione aziendale.

- **obbligo di riservatezza e segretezza:**

il dipendente, in qualità di soggetto autorizzato al trattamento dei dati, ha l'obbligo della riservatezza e del segreto sulle informazioni delle quali venga a conoscenza nel corso delle operazioni di trattamento; deve evitare la comunicazione o la diffusione delle informazioni a soggetti non autorizzati o che non abbiano necessità di conoscere i dati trattati. Si ricorda che l'eventuale violazione degli obblighi ivi considerati può comportare l'applicazione di sanzioni di natura disciplinare e configurare una responsabilità civile e penale secondo quanto previsto dal vigente Codice in materia di protezione dei dati personali;

- **tenuta cartelle e fascicoli:**

Nel caso in cui si ricevano utenti nel proprio ufficio e sulla scrivania siano presenti cartelle o fascicoli, è necessario adottare cautele per garantire la riservatezza dei dati. In particolare, si consiglia di collocare i fascicoli in modo tale da non renderne visibili i contenuti (ad esempio rivoltandoli) oppure di predisporre frontespizi neutri, riportanti solo informazioni generiche o codici identificativi, che non consentano a terzi non autorizzati di risalire all'identità degli interessati.

- **distruzione delle copie cartacee**:

Prima di procedere allo smaltimento della documentazione contenente dati personali, anche appartenenti a categorie particolari, è necessario adottare misure idonee a renderne non comprensibile il contenuto. A tal fine devono essere utilizzati strumenti adeguati, quali distruggidocumenti, oppure, in alternativa, accorgimenti

manuali (ad esempio, lo strappo del documento o la separazione del foglio contenente i dati identificativi dal resto delle informazioni).

- **esercizio dei diritti**

In caso di ricezione di una richiesta di esercizio dei diritti previsti dagli artt. 15-22 del Regolamento (UE) 2016/679, il Direttore o Responsabile della Struttura deve assicurare un riscontro all'interessato entro 30 giorni dalla data di ricezione. Nei soli casi di particolare complessità il termine può essere prorogato fino a un massimo di 60 giorni, informando l'interessato entro i 30 giorni iniziali e motivando la proroga. Qualora un dipendente riceva direttamente un'istanza, è tenuto a non gestirla autonomamente, ma a trasmetterla senza ritardo secondo la procedura interna aziendale prevista.

Per dettagli si rinvia alla vigente procedura per la gestione delle istanze per l'esercizio dei diritti.

Per informazioni complete e costantemente aggiornate sul trattamento dei dati personali e sui Regolamenti aziendali in materia di protezione dei dati, si invita a consultare il sito istituzionale dell'Ente, nell'apposita sezione "Privacy", oppure a contattare il Responsabile della Protezione dei Dati (DPO).

Titolare del Trattamento dei dati (ASL FOGGIA)