Servizio Sanitario Nazionale
Regione Siciliana
VIA MAZZINI, 1 – 91100
TRAPANI
TEL. (0923) 805111 –
FAX (0923) 873745
Codice Fiscale – P. IVA
02363280815

MEMORANDUM

PER I RESPONSABILI E I SOGGETTI DESIGNATI AL TRATTAMENTO DEI DATI

Prescrizioni generali

La normativa sulla Privacy è disciplinata dal Regolamento UE 2016/679, dal D.Lgs. n. 196 del 30 giugno, così come modificato con D.Lgs. 10 Agosto 2018 n.101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016, relativo alla protezione della persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE" e dal Regolamento Aziendale per l'attuazione del Regolamento reperibile sul sito web dell'Azienda (*www.asptrapani.it*).

I responsabili dell'applicazione della normativa sulla Privacy sono i seguenti:

- il "Titolare del trattamento" (art. 4, n. 7, e art. 24 Reg. UE 2016/679): *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*;
- il "Responsabile del trattamento" (art. 4, n. 8, e art. 28 Reg. UE 2016/679): *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*
- *il* "Soggetto designato" (art. 4, n. 10, Reg. UE 2016/679 e art. 2 *quaterdecies*, c.1, D.Lgs. 196/03): persone fisiche espressamente designate che operano sotto l'autorità diretta del Titolare o del Responsabile

Il soggetto designato potrà rivolgersi al Responsabile del Trattamento della propria Struttura di appartenenza, per ulteriori approfondimenti e per ricevere le opportune istruzioni.

Un nuova figura nell'impianto legislativo delineato dal Regolamento UE 2016/679 in materia di protezione delle persone fisiche con riguardo dei dati personali, è rappresentata dal "Responsabile della Protezione Dati" (RDP-DPO), il cui compito è di facilitare l'attuazione della normativa da parte del titolare/responsabile (art. 39, Reg. UE 2016/679).

Fra i compiti del DPO rientrano, infatti:

- l'informazione e la consulenza al titolare, al responsabile e ai soggetti che eseguono il trattamento in merito agli obblighi derivanti dalle disposizioni vigenti;
- la sorveglianza sull'osservanza del Reg. UE 2016/679 e delle altre disposizioni degli Stati membri in materia di protezione dei dati la sensibilizzazione e la formazione del personale che partecipa al trattamento;
- ove richiesto il parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA), ai sensi dell'art. 35, Reg. UE 2016/679;
- la funzione di punto di contatto per gli interessati e per il Garante rispetto a ogni questione attinente l'applicazione del Regolamento (Art. 39, Reg. UE 2016/679).

Cosa sono i dati personali (art. 4, Reg.679/2016)

Il Reg. UE 2016/679 definisce **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.
Tra i dati personali si annoverano:
- «**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*
- «**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;*
- «**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.*

Cosa è il trattamento dei dati personali (art. 4, n.2, Reg.679/2016)
Il Regolamento Europeo **679/2016** definisce "**trattamento dei dati personali**" *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.* E' quindi indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo, contenuti in un archivio o destinati ad essere contenuti in un archivio, sono assoggettati alla normativa Privacy.

Prescrizioni generali sulle modalità di trattamento dei dati (art. 5, Reg.679/2016)
Ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi:
- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- raccolta dei dati personali per finalità determinate, esplicite e legittime compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con dette finalità;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire un'adeguata sicurezza dei dati personali oggetto del trattamento.

Il Reg. UE 2016/679 (art. 5, par. 2) richiede al titolare di rispettare tutti questi principi e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione" (o accountability) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Reg. UE 2016/679, dove si afferma che "*il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento"*.
Sarà cura del soggetto designato effettuare le operazioni di trattamento affidategli nel rispetto delle

disposizioni di legge, verificando, in particolare, che ai soggetti interessati sia stata data l'informativa e ne sia stato ottenuto, ove previsto, il consenso .
Nell'ambito della prescrizione generale, per cui il trattamento deve avvenire secondo i principi di liceità, correttezza e trasparenza, si richiama l'attenzione del soggetto designato sulla necessità di dare prontamente soddisfazione alle richieste che i soggetti interessati possono inoltrare, conformemente a quanto prescritto dall'art. 15 Reg. 679/2016 (*"Diritto di accesso dell'interessato"*), segnalando inoltre tali richieste al Responsabile dei Trattamenti della propria Struttura di appartenenza.

Consenso dell'interessato (artt. 4 e 7, Reg. 679/2016)
Il trattamento in ambito sanitario si fonda sul consenso dell'interessato. Il Reg. UE 2016/679, all'art. 4, *lett.* 11), definisce "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.*
Il titolare deve sempre essere in grado di dimostrare (art. 7, c.1, del Reg. UE 2016/679) che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali ai sensi degli artt.13 e 14 del Reg. UE 2016/679;
- è stato espresso dall'interessato, in modo inequivocabile mediante un atto positivo e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. *L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.*

Occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste da parte dell'Azienda o altre dichiarazioni rese dall'interessato (art. 7, c.2), con riferimento alla modulistica adottata. Infatti, come dettagliatamente descritto, nel caso in cui il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre tematiche (ad esempio il consenso al trattamento terapeutico), la richiesta di consenso al trattamento dati deve essere presentata in modo chiaramente distinguibile dalle altre, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.
Non è ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).Quando il trattamento riguarda le "categorie particolari di dati personali" (art. 9 Reg. UE 2016/679) il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati.
N.B.
Il consenso al trattamento dei dati personali, come sopra specificato, deve essere distinto e separato dal consenso al trattamento terapeutico, che attiene all'esecuzione della prestazione terapeutica richiesta.

I diritti degli interessati (art. 7, 13 Reg. 679/2016)
L'interessato può, in qualsiasi momento, esercitare i seguenti diritti:

- diritto di revocare il proprio consenso in qualsiasi momento, la revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca; prima di esprimere il proprio consenso, l' interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui viene accordato (*ex* art. 7, c. 3, Reg.679/2016);
- diritto di proporre reclamo al Garante per la protezione dei dati personali, che è l'autorità amministrativa indipendente di controllo dello Stato italiano, (*ex* art. 13.2, lett. d,

Reg.679/2016)

- diritto di chiedere al titolare del trattamento (*ex* art. 13, c.2,lett.b ed art. 15 Reg.679/2016) di poter accedere ai propri dati personali;
- diritto di chiedere al titolare del trattamento (*ex* art. 13, c.2,lett.b ed art. 16 Reg.679/2016) di poter rettificare i propri dati personali, ove quest'ultimo non contrasti con la normativa vigente sulla conservazione dei dati stessi e con la necessità di tutelare in caso di contenzioso giudiziario i professionisti sanitari che li hanno trattati;
- diritto di chiedere al titolare del trattamento (*ex* art. 13, c.2,lett.b ed art. 17 Reg.679/2016) di poter cancellare i propri dati personali, ove quest'ultimo non contrasti con la normativa vigente sulla conservazione dei dati stessi e con la necessità di tutelare in caso di contenzioso giudiziario i professionisti sanitari che li hanno trattati;
- diritto di chiedere al titolare del trattamento, (*ex* art. 13, c.2,lett.b ed art. 18 Reg.679/2016), di poter limitare il trattamento dei propri dati personali;
- diritto di opporsi al trattamento, (*ex* art. 13, c.2,lett.b ed art. 21 Reg.679/2016), ove possibile;
- diritto di chiedere al titolare del trattamento la portabilità dei dati (art. 13, c.2,lett.b ed art. 20 Reg.679/2016).

Le Informazioni, Comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12, Reg. 679/2016)

I titolari del trattamento devono rispettare le modalità previste per l'esercizio di tutti i diritti da parte degli interessati.

In primo luogo, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura, tecnica e organizzativa, a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile del trattamento è tenuto a collaborare con il titolare ai fini dell'esercizio di tali diritti (art. 28, par. 3, lettera *e)* Reg.679/2016).

Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (in particolare, art. 11, par. 2 e art. 12, par. 6 Reg.679/2016).

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), pari a 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori.

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, par. 1; art. 15, par. 3).

Spetta al titolare valutare la complessità del riscontro all'interessato applicando, se del caso le regole aziendali in materia di diritto di accesso ai documenti amministrativi.

Misure di sicurezza del trattamento (art. 32, UE Reg.679/2016)

Il titolare e il responsabile del trattamento adottano misure tecniche e organizzative idonee garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Fra tali misure, il Reg. UE Reg.679/2016 menziona la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate.

In ogni caso, il Responsabile della struttura ICT dell'Azienda ha la responsabilità dell'attuazione delle misure minime di sicurezza, ai sensi della Circolare AGIT del 18 aprile 2017 n. 2/2017.

Notifica di una violazione dei dati personali (art. 33, Reg.679/2016): *data breach*

Il titolare dovrà notificare al Garante le violazioni di dati personali di cui viene a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (considerando 85). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

Il responsabile del trattamento, dopo essere venuto a conoscenza della violazione, informa il titolare del trattamento senza ingiustificato ritardo.

Il titolare del trattamento deve in ogni caso documentare le violazioni di dati personali subite nonché le relative circostanze e conseguenze, e i provvedimenti adottati (articolo 33, paragrafo 5).

Trasferimento dei dati all'estero

- Verso Paesi appartenenti all'Unione europea

Non possono esservi limitazioni né divieti alla libera circolazione dei dati personali nell'Unione europea per motivi attinenti alla protezione dei dati (Articolo 1, paragrafo 3 del Regolamento). Pertanto, non vi sono limiti di alcun genere per quanto riguarda i flussi di dati dall'Italia verso altri Stati membri dell'Ue (e dello Spazio Economico Europeo: Islanda, Norvegia, Liechtenstein).

- Verso Paesi non appartenenti all'Unione europea

Il trasferimento di dati personali verso Paesi non appartenenti all'Unione europea è vietato, in linea di principio.

Per maggiori approfondimenti si rinvia agli artt. dal 44 a 49 del Reg.679/2016**.**

Soggetto designato dal Responsabile al trattamento dati

Nella lettera di nomina di ciascun soggetto designato dal Responsabile del Trattamento devono essere indicati i dati personali, genetici, biometrici e relativi alla salute nonché i dati personali relativi a condanne penali e reati che lo stesso designato è autorizzato a trattare, in relazione allo svolgimento delle sue mansioni. Qualora, nello svolgimento della sua attività lavorativa, dovesse venire in possesso di informazioni che esulano da tale autorizzazione, il soggetto designato è invitato a rivolgersi al Responsabile del Trattamento della propria Struttura di appartenenza, per ricevere le istruzioni del caso.

La protezione prevista dal Reg.679/2016 si applica alle sole persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati.

Pertanto, il soggetto designato viene autorizzato al trattamento dei seguenti dati personali:

- dati personali, che consistono in informazioni di carattere anagrafico ed in altre notizie il cui trattamento è necessario in relazione allo svolgimento dell'attività lavorativa, di utenti/pazienti. Tali dati non potranno essere comunicati al di fuori dell'Azienda, tranne nei casi previsti da norme e regolamenti;
- dati genetici, biometrici e relativi alla salute il cui trattamento è necessario in relazione allo svolgimento dell'attività lavorativa, di utenti/pazienti. Tali dati non potranno essere comunicati al di fuori dell'Azienda, tranne nei casi previsti da norme e regolamenti;
- dati che si riferiscono al personale dell'Azienda. Il soggetto designato provvederà a trattare i soli dati che sono strettamente necessari per adempiere agli obblighi previsti dalla legge e per l'elaborazione delle buste paga. In tale contesto, tali dati potranno essere comunicati a consulenti esterni che necessitassero di tali informazioni per curare, per conto dell'Azienda, adempimenti di legge.

La custodia dei dati

I dati personali, necessari per lo svolgimento delle mansioni lavorative, sono, di norma, custoditi negli archivi di varie tipologie (archivi fisici e archivi informatici).

Trattamenti senza strumenti elettronici

Taluni archivi fisici potranno essere ad accesso selezionato, come nel caso della conservazione dei documenti relativi a particolari categorie di dati. Durante i periodi di assenza del soggetto designato tali documenti dovranno essere riposti nell'archivio costituito dagli armadi, muniti di serratura, per cui il soggetto designato può accedervi solo previa richiesta della chiave al Responsabile dei Trattamenti della propria Struttura di appartenenza.

Qualora avesse necessità di accedere a tale archivio dopo l'orario lavorativo, il soggetto designato dovrà rivolgersi al Responsabile, per:

- richiedere la chiave per accedere all'archivio;
- ottenere il "registro degli accessi all'archivio controllato", nel quale dovrà: indicare la data e l'ora dell'accesso;
- descrivere sinteticamente le ragioni;
- apporre la propria firma in caratteri leggibili.

Trattamenti con strumenti elettronici

Nello svolgimento dei suoi compiti, il soggetto designato potrà essere autorizzato ad accedere al Personal Computer a lui reso disponibile dall'Azienda, previa verifica della sua identità, mediante codici di identificazione (*username)* e parola chiave *(password).*

I soggetti designati avranno cura di :

- **non condividere** il proprio codice identificativo personale con altri utenti, salvo i casi espressamente previsti;
- **non cedere** a terzi la propria chiave di autenticazione;
- **non caricare** ed eseguire software di rete o di comunicazione senza previa verifica dello stesso da parte del responsabile ITC;
- **non tentare** di acquisire i privilegi di Amministratore di sistema
- **verificare** l'assenza di virus nei supporti utilizzati
- **memorizzare** i dati di interesse lavorativo ed effettuare il backup periodico su supporti esterni

La parola chiave deve essere:

a) mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia, fatta unicamente eccezione per quanto previsto *sub b)*;

b) comunicata, inserendola in una busta chiusa sigillata sul retro, al Responsabile dei Trattamenti della propria Struttura , o ad altro soggetto da questi delegato.

Si raccomanda di utilizzare i *software* di protezione di cui dispone l'Azienda, le cui specifiche tecniche verranno fornite al soggetto designato, da parte del responsabile ICT ogni volta che vi sono dei significativi aggiornamenti.

Di norma, per lo svolgimento delle mansioni lavorative, al soggetto designato verrà attribuita una casella di posta elettronica aziendale. Si raccomanda di utilizzarla esclusivamente per finalità legate all'attività lavorativa. Giova precisare che sia i messaggi ricevuti, che quelli spediti, saranno leggibili anche da altri soggetti, autorizzati, appartenenti all'Azienda: ciò è necessario per garantire un regolare funzionamento dell'attività aziendale, soprattutto nei giorni di assenza del soggetto.Si rammenta che è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore.

Prescrizione residuale

Per dubbi ed incertezze, il soggetto designato può rivolgersi al Responsabile dei Trattamenti della propria Struttura di appartenenza, per ricevere le opportune istruzioni ed in alternativa al DPO.

Il DPO

Dott.ssa Maria Scarpitta