ASP 4 ENNA AZIENDA SANITARIA PROVINCIALE	REGIONE SICILIANA AZIENDA SANITARIA PROVINCIALE ENNA

DELIBERA N. 53

DEL 23 GEN. 2019

OGGETTO: APPROVAZIONE REGOLAMENTO PER IL TRATTAMENTO E LA TUTELA DEI DATI PERSONALI.

U.O.C. PROPONENTE : COORDINAMENTO STAFF AZIENDALI

PROPOSTA DI DELIBERAZIONE N. 392197

DEL 21 GEN. 2019

RESPONSABILE DEL PROCEDIMENTO	IL DIRETTORE
U.O.S. P.A.C., Anticorruzione, Trasparenza, Privacy (Dr. G. Giarrizzo)	U.O.C. COORDINAMENTO STAFF AZIENDALE (Avv. G. Capizzi)

S.E.F.P.

Si attesta la copertura finanziaria e la compatibilità con il bilancio di previsione vigente.

[ ] come da prospetto allegato (ALL. N. ___) che è parte integrante della presente delibera.

[ ] Autorizzazione n. ___ del ___ C.E. / C.P. ___

IL RESPONSABILE DEL PROCEDIMENTO	IL DIRETTORE DEL S.E.F.P.
COADIUTORE AMMINISTRATIVO Rag. Francesca Giallombardo	DIRETTORE DEL SERVIZIO ECONOMICO FINANZIARIO E PATRIMONIALE Dr.ssa O. Monasteri

22/01/2019

IL DIRIGENTE RESPONSABILE DELLA U.O.C. COORDINAMENTO STAFF AZIENDALI

PREMESSO

Che la disciplina introdotta dal Regolamento europeo per la protezione dei dati personali, Regolamento (UE) 679/2016 (c.d. GDPR), è divenuta direttamente applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018;

Che la principale novità introdotta dal Regolamento consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti, e affida la protezione dei dati al Titolare del trattamento il quale, grazie al principio di responsabilizzazione, potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento (lecito) dei dati personali;

Che l'implementazione del "sistema privacy" delineato dal GDPR implica la necessità di generare nell'organizzazione la piena consapevolezza del rischi inerenti ai trattamenti dei dati e le responsabilità connesse, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero asset informativo di un'organizzazione, con particolare attenzione ai dati sanitari (ivi compresi i dati biometrici e genetici), nonché ai cosiddetti dati sensibili sotto il profilo dei diritti e delle libertà fondamentali dell'individuo;

Che con delibera n. 821 del 05/10/2017 l'Azienda Sanitaria Provinciale di Enna ha già provveduto a confermare quale Responsabile della Privacy aziendale la Dr.ssa Carmela Ghirlanda, già individuata con atto deliberativo n. 935/2013, cui sono stati demandati i compiti esemplificati in via non esaustiva nel citati atto deliberativo;

Che con il medesimo atto deliberativo 821/2017 si è proceduto alla nomina dei componenti del gruppo Privacy aziendale cui è stato demandato il compito di coadiuvare e supportare il Responsabile della Privacy nell'espletamento di tutte le attività discendenti dai compiti attribuiti a tale figura dalla normativa di riferimento;

Che con delibera n. 144 del 24/05/2018 si è provveduto a designare il dipendente Ing. Angelo Di Pasquale nell'incarico di Data Protection Officer (DPO) o Responsabile della Protezione dei Dati, nelle more della definizione delle procedure per l'acquisizione dei servizi di supporto al DPO di cui alla gara CONSIP SPC cloud – lotto 2 Servizi di sicurezza;

Che le attività del DPO troveranno supporto sia nel Responsabile della Privacy aziendale che nel gruppo Privacy aziendale con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda medesima;

Che con delibera n. 634 del 05/10/2018 si è provveduto ad individuare i "Responsabili del trattamento";

Che, nel corso della riunione del "gruppo privacy" tenutasi in data 20/12/2018 (verbale n. 18), si è provveduto a elaborare il nuovo "Regolamento per il trattamento e la tutela dei dati personali all'interno dell'Azienda Sanitaria Provinciale di Enna" adeguato alle previsioni del Regolamento Generale sulla Protezione dei dati o GDPR n. 2016/679;

Che di tale regolamento, composto di n. 32 articoli, fanno parte integrante e sostanziale i seguenti allegati:

- ✓ Procedura per la gestione di Data Breach ai sensi del GDPR (Regolamento Europeo 679/2016) e relativa modulistica per le comunicazioni;
- ✓ Informativa sul trattamento dei dati personali (ai sensi del regolamento (UE) n. 679/2016 e del D. Lgs. n. 101/2018) consenso al trattamento dei dati;
- ✓ Designazione incaricati trattamento dei dati personali (reg. UE 679/2016, D. Lgs. n. 101/2018, D. Lgs. n. 196/2003);
- ✓ Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali vademecum e specifiche istruzioni ai soggetti designati;

- ✓ Vademecum per gli incaricati dei trattamenti;
- ✓ Massimario di conservazione e scarto documenti
- ✓ Atto di nomina a responsabile esterno per il trattamento dei dati personale;

CONSIDERATO

Che l'A.S.P. di Enna ritiene necessario dotarsi di un nuovo regolamento per il trattamento e la tutela dei dati personali aggiornato a seguito delle modifiche normative in materia intervenute con l'introduzione del GDPR n. 2016/679;

Che la Direzione della U.O.C. Coordinamento Staff Aziendali che propone il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è totalmente legittimo e utile per il servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art. 3 del D.L. 23 ottobre 1996, come modificato dalla L. 20 dicembre 1996 n. 639, e che lo stesso è stato predisposto nel rispetto della Legge 6 novembre 2012 n. 190 – Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione – nonché nell'osservanza dei contenuti del Piano aziendale della prevenzione della corruzione 2018/2020;

PROPONE

- ➢ Di approvare il nuovo "Regolamento per il trattamento e la tutela dei dati personali all'interno dell'Azienda Sanitaria Provinciale di Enna" adeguato alle previsioni del Regolamento Generale sulla Protezione dei dati o GDPR n. 2016/679, nel testo elaborato dal Gruppo Privacy nella riunione del 20/12/2018 che, allegato al presente provvedimento, ne costituisce parte integrante e sostanziale;

- ➢ Di approvare, contestualmente, la modulistica informativa, le procedure e le linee guida allegate al superiore Regolamento, consistente nei seguenti documenti:
  - ✓ Procedura per la gestione di Data Breach ai sensi del GDPR (Regolamento Europeo 679/2016) e relativa modulistica per le comunicazioni;
  - ✓ Informativa sul trattamento dei dati personali (ai sensi del regolamento (UE) n. 679/2016 e del D. Lgs. n. 101/2018) consenso al trattamento dei dati;
  - ✓ Designazione incaricati trattamento dei dati personali (reg. UE 679/2016, D. Lgs. n. 101/2018, D. Lgs. n. 196/2003);
  - ✓ Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali vademecum e specifiche istruzioni ai soggetti designati;
  - ✓ Vademecum per gli incaricati dei trattamenti;
  - ✓ Massimario di conservazione e scarto documenti;
  - ✓ Atto di nomina a responsabile esterno per il trattamento dei dati personale

- ➢ Di dare atto che il nuovo regolamento, composto di n. 32 articoli, unitamente alla modulistica allegata, sostituisce quello approvato con delibera n. 558 del 01/03/2010;

Il Dirigente Responsabile dell'U.O.C. Coordinamento Staff Aziendali
Avv. G. Capizzi

L'anno duemiladiciannove il giorno Venti Sei ... del mese di Gennaio nella sede dell'Azienda Sanitaria Provinciale di Enna

IL COMMISSARIO STRAORDINARIO

Dott. Francesco Iudica nominato con Decreto Assessoriale n. 2494 del 18/12/2018 coadiuvato dal Direttore Sanitario, Dott. Emanuele Cassarà e con l'assistenza del Segretario Verbalizzante

VISTI

- ✓ La superiore proposta
- ✓ La Legge Regionale n. 5/2009 e s.m.i.;
- ✓ L'Atto Aziendale adottato con delibera n.429/2017;

Preso atto della suddetta proposta di deliberazione, che qui si intende di seguito riportata e trascritta, quale parte integrante e sostanziale del presente provvedimento;

Preso atto che la Direzione della U.O.C. Coordinamento Staff Aziendale che propone il presente provvedimento, sottoscrivendolo, attesta che lo stesso, a seguito dell'istruttoria effettuata, nella forma e nella sostanza, è totalmente legittimo e utile per il servizio pubblico, ai sensi e per gli effetti di quanto disposto dall'art. 3 del D.L. 23 ottobre 1996, come modificato dalla L. 20 dicembre 1996 n. 639, e che lo stesso è stato predisposto nel rispetto della Legge 6 novembre 2012 n. 190 – Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione – nonché nell'osservanza dei contenuti del Piano aziendale della prevenzione della corruzione 2018/2020;

Acquisito il parere favorevole del Direttore Sanitario;

DELIBERA

- ➢ Di approvare il nuovo "Regolamento per il trattamento e la tutela dei dati personali all'interno dell'Azienda Sanitaria Provinciale di Enna" adeguato alle previsioni del Regolamento Generale sulla Protezione dei dati o GDPR n. 2016/679, nel testo elaborato dal Gruppo Privacy nella riunione del 20/12/2018 che, allegato al presente provvedimento, ne costituisce parte integrante e sostanziale;

- ➢ Di approvare, contestualmente, la modulistica informativa, le procedure e le linee guida allegate al superiore Regolamento, consistente nei seguenti documenti:
  - ✓ Procedura per la gestione di Data Breach ai sensi del GDPR (Regolamento Europeo 679/2016) e relativa modulistica per le comunicazioni;
  - ✓ Informativa sul trattamento dei dati personali (ai sensi del regolamento (UE) n. 679/2016 e del D. Lgs. n. 101/2018) consenso al trattamento dei dati;
  - ✓ Designazione incaricati trattamento dei dati personali (reg. UE 679/2016, D. Lgs. n. 101/2018, D. Lgs. n. 196/2003);
  - ✓ Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali vademecum e specifiche istruzioni ai soggetti designati;
  - ✓ Vademecum per gli incaricati dei trattamenti;
  - ✓ Massimario di conservazione e scarto documenti;
  - ✓ Atto di nomina a responsabile esterno per il trattamento dei dati personale;

- ➢ Di dare atto che il nuovo regolamento, composto di n. 32 articoli, unitamente alla modulistica allegata, sostituisce quello approvato con delibera n. 558 del 01/03/2010;

Di notificare il presente provvedimento al Responsabile della Privacy aziendale ed al Data Protection Officer aziendale, provvedendo, altresì, a dare comunicazione dell'avvenuta approvazione e pubblicazione del

regolamento ai Responsabili del Trattamento per darne e dovuta conoscenza al personale dipendente afferente alle rispettive UU. OO..

Di pubblicare il presente atto sul sito istituzionale aziendale nell'apposita sezione dedicata alla "Privacy" e sul sito intranet aziendale.

IL DIRETTORE SANITARIO
Dr. Emanuele Cassarà

IL COMMISSARIO STRAORDINARIO
Dr. Francesco Iudica

IL SEGRETARIO VERBALIZZANTE
Luisa Tranchida

PUBBLICAZIONE

Si dichiara che la presente deliberazione, su conforme relazione dell'addetto, è stata pubblicata in copia all'Albo Pretorio informatico dell'Azienda Sanitaria Provinciale di Enna, ai sensi e per gli effetti dell'art. 53, comma 2, della L.R. n° 30/93 s.m.i., e dell'art. 32 della L. n. 69 del 18/06/2009

dal 27 GEN 2019 al 10 FEB. 2019

L'incaricato

PER DELEGA DEL DIRETTORE AMMINISTRATIVO
Il Direttore
U.O.C. COORDINAMENTO STAFF AZIENDALE
Avv. G. Capizzi

Notificata al Collegio Sindacale il ..... con nota prot. n°. .....

DELIBERA SOGGETTA AL CONTROLLO

dell'Assessorato Regionale Sanità ex L.R. n° 5/09 trasmessa in data _____ prot. n° _____

SI ATTESTA

che l'Assessorato Regionale Sanità:

- ha pronunciato **l'approvazione** con provvedimento n° _____ del _____
- ha pronunciato **l'annullamento** con provvedimento n° _____ del _____

come da allegato.

Delibera divenuta esecutiva per decorrenza del termine previsto dall'art. 16 della L.R. n° 5/09 dal _____

DELIBERA NON SOGGETTA AL CONTROLLO

- esecutiva ai sensi dell'art. 65 della L.R. n° 25/93, così come modificato dall'art. 53 della L.R. n° 30/93 s.m.i., per decorrenza del termine di 10 gg. di pubblicazione all'Albo, dal 06 FEB 2019
- immediatamente esecutiva dal _____

Enna lì,

IL FUNZIONARIO INCARICATO

_____

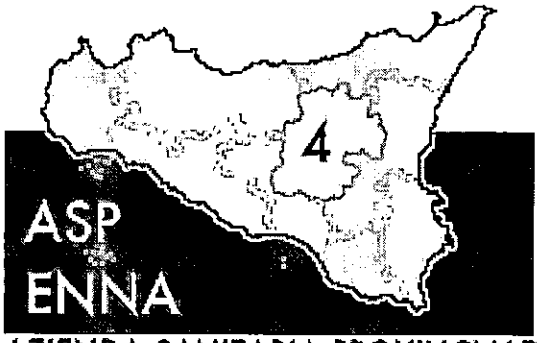
REVOCA/ANNULLAMENTO/MODIFICA

- Revoca/annullamento in autotutela con provvedimento n°. _____ del _____
- Modifica con provvedimento n°. _____ del _____

Enna lì,

IL FUNZIONARIO INCARICATO

_____



AZIENDA SANITARIA PROVINCIALE

Azienda Sanitaria Provinciale di Enna
Viale Diaz n.7/9 94100 Enna
COD. FISC. E P.IVA: 01151150867

REGOLAMENTO PER IL TRATTAMENTO E LA TUTELA DEI DATI PERSONALI ALL'INTERNO DELL'AZIENDA SANITARIA PROVINCIALE DI ENNA

Adeguato al GDPR n.679/2016

PREMESSA

1. Oggetto
2. Dati Personali
3. Trattamento dei dati personali
4. Criteri per l'esecuzione del trattamento dei dati personali
5. Consenso al trattamento dei dati
6. Comunicazione dei dati
7. Titolare del trattamento dei dati personali
8. Data Protection Officer
9. Responsabili del trattamento dei dati personali - ai sensi del codice privacy
10. Incaricati del trattamento dei dati personali - ai sensi del codice privacy
11. Trattamento di dati affidati all'esterno
12. Informativa
13. Diritti dell'interessato
14. Obblighi dell'interessato
15. Referente Aziendale per la Privacy
16. Gruppo Privacy
17. Il Registro dei trattamenti - ai sensi del GDPR
18. Conservazione e sicurezza dei dati
19. Videosorveglianza
20. Pubblicità degli atti e diritto alla riservatezza
21. Diritto di accesso alla documentazione
22. Diritto di accesso civico
23. Accesso alle liste di attesa
24. Rapporti tra diritto d'accesso e riservatezza
25. Cartelle cliniche
26. Misure per il rispetto degli interessati
27. Formazione
28. La semplificazione
29. Abrogazioni
30. Rinvio ed adeguamento
31. Entrata in vigore
32. Modulistica

PREMESSA

Il nuovo quadro normativo, che viene a delinearsi a seguito dell'entrata in vigore del Regolamento UE 2016/679, vede l'introduzione di importanti novità in materia di protezione delle persone fisiche, con riguardo al trattamento dei dati personali.

Il presente Regolamento sulla privacy rappresenta uno strumento di applicazione, nell'ambito dell'organizzazione dell'Azienda Sanitaria di Enna, del **D. Lgs. n. 196/2003** (Codice sulla privacy) *e ss. mm. e ii.*, della normativa sovranazionale di cui al **Reg. UE 2016/679 (GDPR)** e del successivo **D.Lgs. n.101/2018**.

La tutela dei dati personali coincide con la tutela della dignità e della libertà delle persone. Per tale motivo questa Azienda ha posto in essere una serie di azioni ed iniziative che hanno come scopo quello di uniformare tutte le attività e le strutture operative al rispetto dei principi e delle norme del GDPR, rendendo operative le disposizioni di legge sopra richiamate.

L'A.S.P. di Enna si propone di tutelare il diritto alla riservatezza e alla protezione dei dati personali dei terzi, siano questi i cittadini che accedono ai servizi dell'Azienda oppure gli operatori che vi lavorano.

Si impone come necessaria l'immediata adozione di un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza.

Il Titolare del trattamento dei dati individua e nomina i Responsabili, individuati in quei dirigenti che hanno il compito di supportarlo nel garantire il rispetto delle norme a tutela della privacy all'interno del servizio, struttura, U.O.C. o reparto dagli stessi diretto. L'elenco completo dei Responsabili del trattamento è consultabile sul sito web, link "privacy".

Per rafforzare la protezione vengono introdotte numerose e rilevanti novità fondate su un principio di cautela e di *accountability* per il titolare ed i responsabili (valutazione di impatto, registro dei trattamenti, misure di sicurezza, nomina del D.P.O., comportamenti proattivi).

Tutti coloro che, a diverso titolo, operano in nome e per conto dell'Azienda Sanitaria Provinciale di Enna e che trattano dati personali, sono designati quali "incaricati di trattamento" e, pertanto, sono chiamati al rigoroso segreto d'ufficio e ricevono istruzioni operative e specifica formazione.

L'Azienda si propone di garantire un' attività formativa dedicata e finalizzata a consolidare negli operatori la cultura del rispetto della dignità della persona e della riservatezza, a divulgare le indicazioni del Garante, a sviluppare l'adozione di strumenti (sia tecnici che organizzativi) che possano assicurare lo svolgimento delle attività in coerenza con la vigente normativa.

La cultura della privacy necessita di un processo di crescita e rafforzamento tra tutti gli operatori, così come la consapevolezza che gli adempimenti consequenziali non siano un inutile gravame, bensì un valido strumento per un concreto miglioramento della qualità del rapporto con l'utenza.

Una importante finalità da perseguire, attraverso una continua interlocuzione con i Responsabili, è il corretto utilizzo della strumentazione elettronica che andrà ad affiancare, senza sostituire completamente, le forme tradizionali di trattamento.

All'avvento della tecnologia e del progresso che, negli ultimi anni, hanno determinato lo sviluppo degli strumenti telematici a servizio del "fare salute", consegue la necessità di una revisione continua per assicurare il rispetto dei principi fondanti del nuovo GDPR.

I principi di efficienza ed efficacia che connotano la qualità della prestazione sanitaria, non possono e non devono mettere a rischio le libertà fondamentali delle persone.

Altrettanto utile appare sottolineare come l' erogazione di servizi sanitari sia attività che ontologicamente "tratta dati" nell'accezione più vasta del termine: attraverso la raccolta, la registrazione, lo studio delle loro mutazioni qualitative e quantitative, la valutazione, la diagnosi, la cura, la conservazione, la consultazione, l'elaborazione, la cancellazione, l'organizzazione, ecc..
L'erogazione delle prestazioni sanitarie e le molteplici attività amministrative demandate all'A.S.P. di Enna saranno precedute da una fase propedeutica nella quale assumerà preminente importanza l'informativa (ai sensi del GDPR privacy) ed il consenso dell'interessato.

Art. 1 - Oggetto -

Il presente Regolamento contiene disposizioni attuative del D.lgs. 196/03 (Codice Privacy) e del Regolamento UE 2016/679 (GDPR) nell'ambito delle strutture dell'A.S.P. di Enna, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda medesima. L'Azienda adotta idonee e preventive misure di sicurezza, volte a 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 della raccolta. L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 7 del D.lgs. 196/03, come ribaditi all'art. 15 del GDPR.

Art. 2 - Dati Personali -

Costituisce dato personale (art. 4, comma 1, lett. b del D.lgs. 196/03 ed art. 4 del GDPR) qualsiasi informazione riguardante una persona fisica identificata o identificabile anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Il dato sensibile, ai sensi dell'art. 4, comma 1, lett. d) del D.lgs. 196/03, o categoria particolare ai sensi dell'art. 9 del GDPR, è quel dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti politici, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché il dato personale idoneo a rivelare lo stato di salute e la vita sessuale dell'interessato.

Art.3 - Trattamento dei dati personali -

Con l'espressione "trattamento", ai sensi dell'art. 4, comma 1, lett. a), del D.lgs. 196/03 e dell'art. 4, punto 2, del GDPR, deve intendersi qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche se non registrati in una banca dati. Qualunque trattamento di dati personali da parte dell'A.S.P. di Enna è consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2 D.lgs. 196/03), al fine di adempiere a compiti ad essa attribuiti da leggi e regolamenti. E' possibile effettuare trattamenti relativi a dati diversi da quelli sensibili e giudiziari anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente,

fermo restando l'esercizio di funzioni istituzionali. Il trattamento dei dati sensibili è invece consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in relazione ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare di cui all'art. 20, comma 2, del D. Lgs. 196/03. In ottemperanza ai principi di necessità, pertinenza e non eccedenza dei dati, la pubblicazione dei provvedimenti aziendali contenenti dati sensibili avviene previa selezione dei soli dati la cui inclusione nelle deliberazioni medesime sia realmente necessaria per il raggiungimento delle finalità proprie di ciascun provvedimento. I soggetti cui si riferiscono le informazioni di carattere sensibile devono essere individuati attraverso l'utilizzo di codici alfanumerici; ogni dato di natura sensibile o giudiziaria o appartenente a categorie particolari di dati personali, ai sensi dell'art. 9 del GDPR, che possa essere isolato dal contesto del provvedimento, senza comprometterne la necessaria motivazione, è riportato in allegati non costituenti parte integrante del provvedimento medesimo o con il riferimento di protocollo.

Art. 4 - Criteri per l'esecuzione del trattamento dei dati personali -

Ogni trattamento di dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto di ogni tipo di trattamento dovranno essere i soli dati essenziali per lo svolgimento delle attività istituzionali. I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati. E' compito dei Responsabili del trattamento verificare periodicamente la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisca di propria iniziativa. I dati che, anche a seguito di verifiche, risultassero eccedenti, non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene. In ogni caso devono essere adottate misure tecniche tali da garantire che i dati personali o sensibili siano accessibili ai soli incaricati di trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

Art. 5 - Consenso al trattamento dei dati -

L'A.S.P. di Enna tratta i dati idonei a rivelare lo stato di salute: a) con il consenso dell'interessato se il trattamento riguarda dati ed operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato; b) anche senza il consenso dell'interessato, ma previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività. Nell'ambito di attività istituzionali c.d. "amministrative", invece, non vi è la necessità di richiedere il consenso dell'interessato, fermo restando il rispetto dell'obbligo dell'informativa.

Art. 6 - Comunicazione dei dati -

Qualunque trattamento di dati personali, da parte di soggetti pubblici, è consentito soltanto per lo svolgimento delle funzioni istituzionali.

La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa, quando è prevista da una norma di legge o di regolamento e, in difetto, quando la stessa è, comunque, necessaria per lo svolgimento delle funzioni istituzionali dell'Azienda.

La comunicazione da parte di un soggetto pubblico a privati o ad enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse, unicamente quando sono previste da una norma di legge o di regolamento.

Fermo restando quanto previsto dal presente regolamento, la comunicazione dei dati personali, inclusi quelli sensibili, trattati, per disposizione di legge o di regolamento o, comunque, per il perseguimento di attività istituzionali, tra le diverse strutture organizzative aziendali, costituisce compito istituzionale e non richiede, pertanto, l'adozione di specifiche formalità, da parte delle strutture stesse.

E' fatta salva, comunque, la comunicazione o la diffusione dei dati, che siano richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

I dati idonei a rivelare lo stato di salute, non possono essere diffusi.

I dati personali idonei a rivelare lo stato di salute dell'interessato possono essere noti a quest'ultimo, per il tramite del medico dell'Azienda, competente in relazione ai provvedimenti organizzativi aziendali, ovvero per il tramite del medico di fiducia dell'interessato da lui designato, o del medico che ha prescritto il ricovero o gli accertamenti.

Il Responsabile del trattamento dati può autorizzare, per iscritto, gli esercenti le professioni sanitarie, diversi dai medici, che, nell'espletamento dei propri compiti, intrattengono diretti rapporti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi risultati all'interessato; l'autorizzazione è, in tal caso, effettuata, in sede di designazione dei predetti esercenti, quali incaricati del trattamento dei dati.

Nell'eventualità che l'interessato si trovi in stato di impossibilità fisica, incapacità di agire o di incapacità di intendere e di volere, le comunicazioni di cui ai commi precedenti, sono rese a chi dimostri, anche mediante autocertificazione, resa ex art.46, D.P.R. n.445/2000, di esercitare legalmente la potestà, ovvero di essere un prossimo congiunto, un familiare, un convivente, o, in loro assenza, il responsabile della struttura presso cui dimora.

In occasione delle prestazioni di pronto soccorso o durante il ricovero, le informazioni di cui sopra possono essere note anche a soggetti diversi dall'interessato, dietro specifico consenso scritto di quest'ultimo.

Art. 7 - Titolare del trattamento dei dati personali -

Il Titolare del trattamento, ai sensi dell'art. 4, comma 1, lett. f) del D.lgs. 196/03, è l'Azienda Sanitaria Provinciale di Enna, rappresentata dal Direttore generale, in qualità di legale rappresentante dell'Azienda stessa, con sede in Viale A. Diaz n. 7/9 in Enna.

Il Titolare, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza, si avvale, in particolare, anche se non in via esclusiva, per quanto attiene al principio di

"responsabilizzazione" introdotto al p. 2 dell'art. 5 del GDPR, della figura del responsabile del trattamento.

Il Titolare, anche avvalendosi della collaborazione del Referente aziendale privacy, provvede:

a) a richiedere al Garante per la protezione dei dati personali l'autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'obbligo di notificazione e comunicazione;
b) a nominare con proprio atto i responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy , all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
c) a nominare il referente privacy e l'amministratore di sistema;
d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
e) mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al presente Regolamento.

Art. 8 - Data Protection Officer (di seguito D.P.O.) -

Il DPO, ai sensi degli art. 37, 38 e 39 del GDPR, provvede a:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il D.P.O. deve: i) essere in possesso di un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, ii) adempiere alle sue funzioni in totale indipendenza ed in assenza di conflitti di interesse, iii) operare alle dipendenze del titolare del trattamento oppure sulla base di un contratto di servizio.

Il D.P.O. è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Art. 9 - Responsabili del trattamento dei dati personali

I Responsabili del trattamento dei dati personali compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di protezione dei dati; in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate nel regolamento privacy elaborato dall'Azienda. Ogni Responsabile del trattamento dei dati è nominato per iscritto dal Titolare del trattamento che all'uopo, al momento formale della nomina (deliberazione di nomina) delega il Servizio preposto alla sottoscrizione del contratto individuale di lavoro. Le Aziende hanno da sempre ritenuto opportuno che i Responsabili di Trattamento siano individuati fra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. A tal fine si è definito che i Responsabili dovessero e potessero essere individuati in coloro che sono chiamati a ricoprire ruoli gestionali quali i Direttori di struttura complessa o semplice dipartimentale. L'elenco completo dei Responsabili del Trattamento è rinvenibile presso la sezione privacy del sito WEB aziendale e sulla Intranet.

Art. 10 - Incaricati del trattamento dati

Chiunque tratti dati su istruzione di Titolare e Responsabile è designato, per iscritto, incaricato di trattamento. In particolare sono identificati incaricati, dipendenti e collaboratori ed in generale tutti coloro che, all'interno dell'Azienda e su mandato specifico della stessa, siano autorizzati, nell'esercizio delle rispettive funzioni, ad effettuare operazioni di trattamento di dati.

Ogni incaricato, a seconda della natura del rapporto in essere con l'A.S.P. di Enna, ha accesso ai soli dati la cui conoscenza sia strettamente necessaria al raggiungimento degli obiettivi propri del rapporto di lavoro. Gli Incaricati, devono eseguire i trattamenti di dati secondo le disposizioni loro date dal Responsabile del trattamento, dalle iniziative formative specifiche e dal presente regolamento. Tale momento decorre - come per i Responsabili - dal momento della sottoscrizione del singolo contratto individuale. L'interlocuzione tra gli incaricati, i responsabili, il referente della privacy ed il Gruppo Privacy e la formazione specifica consentirà a seconda dei rispettivi profili di arricchire o di approfondire le ulteriori istruzioni specifiche che ogni Responsabile riterrà di dover fornire ai propri collaboratori.

Art. 11 - Trattamento di dati affidati all'esterno -

Agli Enti, agli organismi, agli altri soggetti pubblici e privati esterni all'Azienda, ai quali siano affidati attività o servizi, con esclusivo riferimento alle connesse operazioni di trattamento di dati, viene attribuita la qualità di Responsabile ai sensi dell'art. 29 del D.lgs. 196/03. L'elenco di tali contratti deve essere inserito nel Registro dei Responsabili esterni di trattamento e nell'apposita sezione del sito WEB.

Art. 12 - Informativa -

L'informativa è l'elemento necessario e fondamentale per la liceità di ogni forma di trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività specifiche che sono poste in essere. L'informativa è sempre dovuta a prescindere

dall'obbligo di acquisizione del consenso. Essa deve contenere gli elementi tassativamente indicati dall'art. 13 del D.lgs. 196/03 e più specificatamente:

- ✓ le finalità e le modalità con le quali vengono trattati i dati;
- ✓ l'obbligatorietà o meno del conferimento dei dati;
- ✓ le conseguenze di un eventuale rifiuto a fornire i dati;
- ✓ i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- ✓ i diritti di cui all'articolo successivo;
- ✓ gli estremi identificativi del Titolare e del Responsabile di trattamento.

La predetta informativa può essere resa anche tramite affissione di appositi manifesti nei locali di accesso all'utenza, secondo procedure e attraverso modelli o modulistica.

Art. 13 - Diritti dell'interessato -

Secondo quanto disposto dall'art. 7 del D.lgs. 196/03, nonché dal Capo III del GDPR, l'interessato ha diritto, a cura del Titolare o del Responsabile,:

1. di ottenere senza ritardo la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
2. di ottenere l'indicazione: a) dell'origine dei dati personali trattati; b) delle finalità e delle modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del Titolare; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati;
3. di fare richiesta di: a) aggiornamento, rettifica ovvero, qualora vi abbia interesse, integrazione dei dati; b) cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) attestazione che le operazioni di cui ai precedenti punti a) ed b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato;
4. l'interessato ha, inoltre, il diritto di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati che lo riguardano, ancorché pertinenti allo scopo della raccolta.

Nel caso in cui intenda presentare istanza per fatti inerenti al trattamento dei propri dati personali, l'utente dovrà rivolgere istanza scritta alla Direzione Generale dell'A.S.P. di Enna.

L'interessato, nell'esercizio dei diritti sopra riportati, può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

Art. 14 - Obblighi dell'interessato -

L'Utente dell'Azienda è obbligato a fornire i dati personali o sensibili strettamente necessari ai fini istituzionali dell'Ente per potere accedere alle prestazioni richieste.
Sono fatti salvi i casi d'urgenza o di impossibilità temporanea a comunicare i dati.

L'interessato che si oppone al trattamento dei propri dati deve indicare espressamente i motivi che legittimano la richiesta. L'opposizione potrà essere accolta solo qualora non sia in contrasto con le disposizioni di legge o con le finalità istituzionali dell'Azienda.

Art. 15 - Referente Aziendale per la Privacy

Il Referente aziendale per la privacy è nominato con atto formale del Direttore generale e svolge, anche con l'ausilio del Gruppo Privacy previsto dall'articolo 16 del presente Regolamento, i seguenti compiti:

a) assiste il Titolare del trattamento nello svolgimento degli adempimenti di cui all'art. 7, comma 3, del presente Regolamento;
b) assiste il Titolare, i responsabili del trattamento ed il D.P.O., nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati, per quanto riguarda gli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
c) collabora con il Titolare del trattamento per la predisposizione del documento di valutazione d'impatto sulla protezione dei dati e per la definizione del Registro delle attività di trattamento, in collaborazione con l'amministratore di sistema e con le altre strutture competenti dell'Azienda, nonché per gli eventuali aggiornamenti o adeguamenti del documento stesso;
d) vigila sull'osservanza del presente Regolamento e fornisce consulenza ai responsabili dei trattamenti sulle problematiche riguardanti la normativa in materia di riservatezza dei dati personali;
e) in collaborazione con il Responsabile del trattamento dei dati, fornisce informazioni all'utenza relativamente all'applicazione della normativa in materia di riservatezza e protezione dei dati personali;
f) cura l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno dell'Azienda per l'applicazione della normativa vigente e del presente Regolamento;
g) effettua i necessari approfondimenti per l'applicazione della normativa in materia di protezione dei dati personali;
h) propone interventi di formazione a livello aziendale, in tema di normativa sulla riservatezza e protezione dei dati.

Art. 16 - Gruppo Privacy (G.P.) -

L'Azienda individua un gruppo di professionisti che possa supportare il Titolare ed il Referente aziendale per la Privacy per la messa a regime di ogni misura risulti necessaria e/o utile al mantenimento di un buon grado di adeguamento alle norme del Codice privacy ed alle nuove norme contenute nel GDPR. Il G.P. è un gruppo di lavoro permanente composto di diverse professionalità, portatrici di esperienza e conoscenza specifica dei vari settori di gestione aziendale e conoscenza della complessa organizzazione aziendale, nella sua interezza, e delle relazioni che intercorrono tra le diverse strutture concorrenti ai fini di sanità pubblica. Il G.P. garantisce al Titolare, al Referente aziendale per la Privacy ed al D.P.O. il necessario supporto per lo svolgimento dei compiti loro assegnati. Il G.P., nominato con atto del Titolare, è chiamato a coadiuvare il D.P.O. nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per

quanto riguarda gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali. Concorre a promuovere l'osservanza del regolamento aziendale sulla privacy fornendo la necessaria consulenza in ordine alle problematiche in tema di protezione dei dati; mantiene in modo archivisticamente corretto la produzione di normativa interna in materia di trattamento dei dati e concorre ad aggiornare le iniziative di formazione interna specifica.

Art. 17 - Il Registro dei trattamenti - ai sensi del GDPR -

L'Azienda dispone di un registro dei trattamenti di dati personali pubblicato e periodicamente aggiornato sul sito web nell'apposita sezione "privacy". Il registro contiene la rilevazione dei trattamenti dei dati suddivisi per tipologie come presupposto necessario per adempiere agli obblighi di legge. E' tenuto a cura del D.P.O. in collaborazione con i Responsabili del trattamento; esso viene aggiornato qualora vengano comunicati da parte del Titolare o dei Responsabili del trattamento casi di attivazione di un nuovo trattamento, variazioni significative dei trattamenti già in essere, o cessazione di un trattamento in essere.

Art. 18 - Conservazione e sicurezza dei dati -

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo tale da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distribuzione o di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

I Responsabili del trattamento dei dati, sono tenuti ad impartire le necessarie istruzioni al personale incaricato, affinché venga costantemente garantito lo standard minimo di sicurezza al fine di meglio garantire il diritto di riservatezza degli utenti.

L'accesso agli archivi aziendali deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura.

Con riferimento agli archivi aziendali la responsabilità della conservazione e sicurezza dei medesimi spetta al responsabile competente per i dati oggetto del trattamento.

Art. 19 – Videosorveglianza -

L'installazione di nuovi impianti di videosorveglianza nell'Azienda è consentita, solo dopo attenta valutazione sulla proporzionalità fra lo strumento impiegato e gli scopi perseguiti (assistenza e cura dei pazienti ricoverati, sicurezza delle persone e delle attrezzature) e, in ogni caso, quando altre misure possibili siano concretamente insufficienti o inattuabili.

Trova comunque applicazione, circa il divieto di controllo del lavoratore a distanza, l'intero dispositivo dell'art. 4, legge n.300/70 e s.m.i..

Art. 20 – Pubblicità degli atti e diritto alla riservatezza -

L'Azienda, salvo diverse disposizioni di legge, garantisce il diritto alla riservatezza dei dati personali/giudiziari, contenuti negli atti amministrativi pubblicati nell'apposito albo, mediante la non diretta identificabilità dei soggetti, cui tali dati si riferiscono.

I responsabili delle strutture organizzative che propongono una deliberazione o che adottano un provvedimento dirigenziale con il supporto tecnico dei relativi responsabili del procedimento verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dal **GDPR**, che l'inclusione nel testo e nell'oggetto di dati personali sia realmente necessaria per perseguire le finalità dell'atto stesso.
Devono essere privilegiate modalità di redazione degli atti che prevedono l'utilizzo di dati anonimi o non direttamente identificativi, quali codici o altri riferimenti se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.
L'Azienda garantisce la riservatezza dei dati personali in sede di pubblicazione all'Albo delle deliberazioni o di altri atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. Gli individui cui afferiscono le informazioni di carattere personale/giudiziario debbono, in particolare, essere individuati, nell'oggetto del relativo provvedimento, attraverso le sole iniziali di nome e cognome.

Art. 21 - Diritto di accesso alla documentazione -

Nel caso in cui nel corso della procedura di accesso ai documenti amministrativi venissero in evidenza problematiche connesse alla tutela della privacy di soggetti terzi, sarà compito del responsabile del trattamento, valutare caso per caso la possibilità di esercitare il diritto di accesso.
Salvo quanto previsto all'art. 6 e fatti salvi gli atti sottratti all'accesso per norma di legge o di regolamento, l'Azienda garantisce il diritto di accesso alla documentazione amministrativa, ai sensi dell'articolo 22 della L. 241/90 e s.m.i. e del Regolamento Aziendale approvato con delibera n° 2043/2010 aggiornato con delibera n° 166 del 30.05.2018, nei limiti previsti, in particolare, agli artt. 11 e 24 del Titolo II del predetto Regolamento.
Qualora l'istanza di accesso riguardi documenti contenenti dati idonei a rivelare lo stato di salute o la vita sessuale di un terzo, l'accesso è consentito a condizione che ciò si renda necessario per far valere o difendere in sede giudiziaria una situazione giuridicamente rilevante di rango almeno pari ai diritti del terzo, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso stesso.

Art. 22 - Diritto di accesso civico -

Nel caso in cui nel corso della procedura di accesso civico ai sensi del D. Lgs 33/2013 e s.m.i, venissero in evidenza problematiche connesse alla tutela della privacy di soggetti terzi, l'accesso civico generalizzato potrà essere negato, differito o consentito solo parzialmente, laddove possa arrecare un pregiudizio concreto alla protezione dei dati personali in conformità con la disciplina legislativa in materia e secondo quanto previsto agli artt. 24, 25 e 26 del Titolo II del Regolamento Aziendale disciplinante il diritto di accesso approvato con delibera n° 2043/2010 ed aggiornato con delibera n° 166 del 30.05.2018.

Il responsabile del trattamento dei dati interessato dall'accesso civico generalizzato dovrà operare la valutazione caso per caso al fine di verificare la sussistenza o meno del pregiudizio nel rispetto della normativa di settore, in particolare delle Linee Guida adottate dall'Autorità Nazionale Anticorruzione d'intesa con il Garante di cui alla delibera n. 1309 del 28/12/2016.

Art.23 – Accesso alle liste di attesa

Per le finalità di cui al comma 8 dell'articolo 3 della legge 23 dicembre 1994, n. 724, e fatto salvo il diritto di accesso da esercitarsi ai sensi dell'art. 21 del presente regolamento, l'interessato ha diritto conoscere, anche tramite un proprio delegato da identificarsi come per legge, il numero di posizione che occupa nelle liste delle prestazioni ambulatoriali, di diagnostica strumentale e di laboratorio, dei ricoveri ospedalieri e nelle altre liste di attesa, ma non può essere messo a conoscenza dei nominativi delle persone che lo precedono o che lo seguono nell'elenco.

Fuori dei superiori casi, le informazioni sulle prenotazioni e sui relativi tempi di attesa sono fornite ai soggetti che vi abbiano interesse, a norma della L.241/90 e s.m.i., e del Regolamento Aziendale approvato con delibera n° 2043/2010 aggiornato con delibera n° 166 del 30.05.2018, con la salvaguardia del diritto alla riservatezza delle persone.

Art. 24 - Rapporti tra diritto d'accesso e riservatezza -

I presupposti, le modalità, i limiti per l'esercizio del diritto d'accesso a documenti amministrativi, contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla L. 241/90 e s.m.i. e dalle altre disposizioni di legge in materia, nonché dal regolamento aziendale che disciplina il diritto di accesso, anche per ciò che concerne i dati personali e giudiziari e le operazioni di trattamento, eseguibili in adempimento di una richiesta di accesso.

In tema di riservatezza, diritti dell'interessato e dell'eventuale contro interessato, si richiamano, in particolare, i precedenti artt. 21, 22 e 23.

Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Art. 25 - Cartelle cliniche -

La cartella clinica costituisce, ad ogni effetto di legge un atto pubblico.

Essa deve essere redatta in forma intelligibile e coerentemente ai requisiti di veridicità e completezza.

Ogni annotazione va in essa trascritta, contemporaneamente all'evento descritto.

Nella cartella clinica, i dati relativi al paziente debbono chiaramente distinguersi da quelli eventualmente riguardanti altri interessati, ivi comprese le informazioni relative ai nascituri.

Le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente.

Continuano, comunque, ad applicarsi tutte le restanti disposizioni di legge, in ordine alla loro compilazione e conservazione.

Eventuali richieste di presa visione o di rilascio di copia di cartella clinica e dell'acclusa scheda di dimissione ospedaliera, da parte di soggetti diversi dall'interessato, possono

essere accolte in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

- ✓ di far valere o di difendere un diritto in sede giudiziaria, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
- ✓ di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante, di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile.

Art. 26 - Misure per il rispetto degli interessati -

Presso i locali dell'Azienda, a cura di ciascun Responsabile del trattamento dati, sono adottate procedure, quali l'adozione di opportuna segnaletica per delineare le distanze di cortesia, atte a garantire la riservatezza degli utenti, in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, ecc.) od amministrative (rimborsi o indennità).

I Responsabili del trattamento dati sono, inoltre, chiamati ad adottare misure idonee ad assicurare che le informazioni sanitarie, rese agli utenti verbalmente (chiamata dei pazienti, indagine anamnestica, elaborazione diagnostica, colloqui con i familiari ecc.) o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.

E' possibile dare notizia, anche per telefono, sul passaggio o sulla presenza di una persona al pronto soccorso, solo a terzi legittimati (parenti, familiari, conviventi), così come solo a terzi legittimati (familiari, conoscenti, personale volontario) è possibile fornire informazioni sui degenti, quanto alla loro presenza all'interno dei reparti.

In entrambe le ipotesi, va, comunque, rispettata un'eventuale diversa volontà espressa, al momento dell'accettazione o del ricovero, dall'interessato cosciente e capace. Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.

Il trattamento dei dati idonei a rivelare le convinzioni religiose non può avvenire in maniera sistematica e preventiva ma solo su richiesta dell'interessato o, qualora lo stesso sia impossibilitato, di un terzo legittimato quale ad esempio un familiare, un parente un convivente.

Art. 27 – Formazione -

L' Azienda, organizza, di norma, nell'ambito del piano annuale di formazione del personale, interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

L'intervento formativo predisposto dall'Azienda ricomprende anche le azioni generali di informazione e formazione attivate nell'ambito del Sistema Aziendale Privacy .

Art. 28 - La semplificazione -

L'Azienda, considerando la semplificazione quale fattore principale su cui far leva per il perseguimento dei fondamentali principi di buon andamento, efficienza, efficacia ed economicità dell'attività amministrativa, promuove azioni e progetti volti alla semplificazione dei processi e delle procedure interne rivolti all'esecuzione di adempimenti normativi e regolamentari in materia di protezione dei dati personali.

Art. 29 – Abrogazioni -

Sono abrogate tutte le disposizioni aziendali in contrasto con quelle previste dal presente regolamento.

Art. 30 - Rinvio ed adeguamento -

Per quanto non previsto dal presente regolamento si applicano le disposizioni contenute nel GDPR e nei provvedimenti emanati dal Garante.

Gli eventuali interventi del legislatore nazionale e regionale successivi all'entrata in vigore del presente regolamento, di modifica del quadro normativo sulla riservatezza e protezione dei dati personali, producono un automatico adeguamento del presente regolamento con successivo e necessario aggiornamento con le modalità previste per l'approvazione delle procedure aziendali.

Il presente Regolamento sarà sottoposto ad aggiornamento periodico, in linea con le novità normative, le pronunce giurisprudenziali e con le direttive del Garante Privacy.

Art. 31 - Modulistica -

L'Azienda si dota di apposita modulistica di informativa, procedure e linee guida di seguito elencata ed allegata al presente Regolamento. Tale modulistica sarà periodicamente aggiornata a cura del Referente Aziendale per la Privacy in collaborazione con i responsabili del trattamento.

Eventuali ulteriori modelli da adottare per specifiche esigenze organizzative delle strutture saranno predisposti dai responsabili del trattamento, in relazione alle rispettive competenze, sentito il Referente Aziendale per la Privacy.

- ✓ Procedura per la gestione di Data Breach ai sensi del GDPR (Regolamento Europeo 679/2016) e relativa modulistica per le comunicazioni;
- ✓ Informativa sul trattamento dei dati personali (ai sensi del regolamento (UE) n. 679/2016 e del D. Lgs. n. 101/2018) consenso al trattamento dei dati;
- ✓ Designazione incaricati trattamento dei dati personali (reg. UE 679/2016, D. Lgs. n. 101/2018, D. Lgs. n. 196/2003);
- ✓ Elenco degli specifici compiti e funzioni attribuiti e connessi al trattamento dei dati personali vademecum e specifiche istruzioni ai soggetti designati;
- ✓ Vademecum per gli incaricati dei trattamenti;
- ✓ Massimario di conservazione e scarto documenti;
- ✓ Atto di nomina a responsabile esterno per il trattamento dei dati personale.

Art. 32 - Entrata in vigore -

Il presente Regolamento, adottato con deliberazione del Direttore Generale dell'Azienda, entra in vigore dalla data di esecutività della stessa.

REGIONE SICILIANA
AZIENDA SANITARIA PROVINCIALE DI ENNA
C.F. 01151150867 - www.asp.enna.it
Viale A. Diaz n. 7/9

Procedura per la gestione di *Data Breach* ai sensi del GDPR (Regolamento Europeo 679/2016).

Sommario

1. Premessa

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

2. Scopo del documento e ambito di applicazione

Il presente documento si prefigge lo scopo di indicare ai Responsabili del trattamento dell'Azienda Sanitaria Provinciale di Enna le opportune modalità di gestione del *data breach*, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016.
In questo documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:
- modalità e profili di segnalazione al Titolare per il tramite del Responsabile del trattamento;
- modalità e profili di segnalazione all'Autorità Garante;
- valutazione dell'evento accaduto;
- eventuale comunicazione agli interessati;

3. Definizioni

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 (art. 4, punto 1 GDPR).

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 (art. 4, punto 2 GDPR).

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia digitalizzato o meno, centralizzato, decentralizzato o ripartito in modo funzionale o geografico (art. 4, punto 6 GDPR).

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 (art. 4, punto 7 GDPR). In questo contesto, è titolare del trattamento l' Azienda Sanitaria Provinciale di Enna.

Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

Delegato del trattamento: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda sanitaria che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.

Autorizzato al trattamento: la persona fisica, espressamente designata, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10).

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 (art. 4, punto 8 GDPR).

Violazione dei dati personali (c.d. 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 (art. 4, punto 12 GDPR).

4. Normativa e documenti di riferimento

- *Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34*
- *Guidelines on Personal data breachnotification under Regulation 2016/679 – article 29 data protectionworking party (Adopted on 3 October 2017 – as last Revised and Adopted on 6 February 2018)*

5. Gestione del *data breach* interno alla struttura

5.1 Premesse

È necessario l'Azienda dia notizia a tutti gli operatori in merito alla presente procedura mediante idonea comunicazione.

5.2 Modalità e profili di notifica all'Autorità Garante Privacy

Ogni operatore aziendale autorizzato a trattare dati, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il Responsabile del trattamento.
Quest'ultimo, valutato l'evento, avvalendosi, nel caso, del Gruppo privacy, del DPO e di eventuali altre professionalità necessarie per la corretta analisi della situazione, se confermate le valutazioni di potenziale *data breach*, lo segnala senza ingiustificato ritardo al titolare del trattamento tramite le consuete modalità di gestione dei flussi documentali già in uso nell'Azienda.

Per "ingiustificato ritardo" si considera la notizia pervenuta al titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile del trattamento.

Ai fini di una corretta classificazione dell'episodio, il Responsabile del trattamento utilizzerà lo schema di scenario di *data breach*, allegato alla presente procedura .
Pertanto, sulla scorta delle determinazioni raggiunte, il Responsabile del trattamento predispone l'eventuale comunicazione all'Autorità Garante, a firma del titolare, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali, utilizzando il modello **(ALL. 1).**
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del il Responsabile del trattamento.

6. Gestione del *data breach* esterno alla struttura

Ogni qualvolta l'Azienda/titolare del trattamento si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach.*
Rimane salva la possibilità che sia il responsabile del trattamento ad effettuare una notifica per conto del titolare del trattamento, se il titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del GDPR e secondo le modalità previste dal superiore punto **5.2.**.
La responsabilità legale della notifica rimane in capo al titolare del trattamento.

7. Modalità di comunicazione agli interessati

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.
Il Responsabile al trattamento predispone l'eventuale comunicazione all'interessato/agli interessati, a firma del titolare, da inviarsi nei tempi e nei modi che lo stesso, anche attraverso la funzione

consulenziale del DPO, individuerà come più opportuna come specificato nell'art. 34 del GDPR e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante, utilizzando il modello (**ALL.2**).

8. Schema di valutazione scenari – *data breach*

Di seguito sono illustrati alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di *data breach* all'Autorità Garante.

Tipo di Breach	Definizione	Estensione minima / Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. • Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente. • Incendio di archivio cartaceo delle cartelle cliniche. • Distruzione di campioni biologici.	• Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia). • Rottura di un PC che non contiene dati personali originali (in unica copia). • Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe	Caratteristiche: • Dati non recuperabili o provenienti da procedure non ripetibili. • Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla	• Smarrimento di chiavetta USB contenente dati originali. • Smarrimento di fascicolo cartaceo personale del dipendente.	• Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa.

	possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.		
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibil-mente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interes-sato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Caratteristiche: • Modifiche sistematiche su più casi. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup. • Azione involontaria, o fraudolente, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	• Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery • Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile • Modifica di un documento non ancora validato dal proprio autore.
	Un insieme di dati personali (e riconducibili			• Il medico sul proprio sistema dipartimentale

Divulgazione non Autorizzata	all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. • Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet. • Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	• Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi. • Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico.	• Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi. • Accesso non autorizzato di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale.	• Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal	• Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso.

	involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.		Backup. • cancellazione accidentale dei dati da parte di una persona non autorizzata. • perdita della chiave di decrittografia di dati crittografati in modo sicuro. • irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve.	

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

I casi di *data breach* per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach,* ma è considerato un normale errore procedurale (esempio l'invio informatico di un referto in cui il testo del referto è di un paziente mentre l'anagrafica è di un altro). Questo poiché:

- chi riceve non può sapere a quale paziente fisico è riferito il testo;
- il paziente fisico non è danneggiato poiché nessuno riferimento alla sua persona è stato diffuso.

9. Registro delle violazioni

Il titolare del trattamento cura l'aggiornamento del registro delle violazioni, ai sensi dell'art. 33, comma 5 del GDPR.

ALLEGATO 1

REGIONE SICILIANA
AZIENDA SANITARIA PROVINCIALE DI ENNA
Viale Armando Diaz n. 7/9 - 94100 ENNA
C.F. 01151150867
www.asp.enna.it
Pec: protocollo.generale@pec.asp.enna.it

Prot. n. _____ **Enna**.....

OGGETTO: NOTIFICA DI VIOLAZIONE DATI PERSONALI (DATA BREACH).

Spett.le Garante Privacy Italia
Piazza di Monte Citorio n. 121
00186 Roma
www.gpdp.it - www.garanteprivacy.it

E-mail: garante@gpdp.it
Fax: (+39) 06.69677.3785
Centralino telefonico: (+39) 06.69677.1

Egregio Garante Privacy,
ai sensi dell'articolo 33 del Reg. Ue 2016/679 , sono a inviarVi la seguente notifica di violazione dei dati.

La natura della violazione è la seguente :
[*descrivere la violazione in modo, con l'indicazione di data e ora.*]

Questa violazione riguarda i dati personali di [*indicare il numero degli interessati*] (*indicare la descrizione della categoria degli interessati i cui dati sono stati violati*) e [*non coinvolge/coinvolge*] speciali categorie di dati personali.

Le probabili conseguenze della violazione dei dati sono le seguenti:
[*indicare le conseguenze della violazione*]

Al fine di evitare una ripetizione della violazione oggetto di questa comunicazione, [*Nome organizzazione*] ha attivato le seguenti attività:
[*elencare il piano per affrontare e risolvere la violazione, comprese le riunioni degli esperti chiamati a risolvere il problema, le indagini avviate , le azioni correttive e le future modifiche al*

flusso di dati che ha subito la violazione.]

Ulteriori informazioni su questa violazione possono essere richieste al nostro [*DPO*] contattabile ai seguenti recapiti:
[*Indicare email, telefono, indirizzo del DPO*]

Cordiali saluti,

[*Nome e cognome*]
[*Funzione aziendale*]
[*Recapiti di contatto*]

ALLEGATO 2

REGIONE SICILIANA
AZIENDA SANITARIA PROVINCIALE DI ENNA
Viale Armando Diaz n. 7/9 - 94100 ENNA
C.F. 01151150867
www.asp.enna.it
Pec: protocollo.generale@pec.asp.enna.it

Prot. n. _____ **Enna**.....

OGGETTO: MODELLO DI COMUNICAZIONE DI DATA BREACH AGLI INTERESSATI.

AL SIG. .....

.....

.....

Gentile **[Nome dell'interessato]**

Si comunica che, purtroppo si è verificata una violazione dei suoi dati personali.

Come previsto dal Reg.to UE 2016/679 abbiamo notificato questa violazione al Garante Privacy.

Abbiamo incaricato esperti di sicurezza informatica ed esperti legali per ridurre ulteriormente tale esposizione dei tuoi dati personali.

Cosa è accaduto

Riteniamo che la seguente sequenza temporale di eventi abbia avuto luogo portando alla violazione segnalata

- *[Elencare la cronologia degli eventi. Non è necessario esporre informazioni sensibili sull'organizzazione a meno che non sia cruciale nel descrivere la violazione.]*

Sono stati coinvolti i seguenti dati personali:

- *[Elencare i tipi di dati personali. Ad esempio, Nome, Cognome, ecc]*

Cosa significa questo per lei

Considerando la natura della violazione e i tipi di dati personali coinvolti, riteniamo che le conseguenze per lei siano:

- [*Cerca di elencare le azioni che l'interessato dovrà approntare*]

Come eviteremo in futuro tale problematica

Al fine di evitare che tale violazione si verifichi nuovamente e di ridurre al minimo l'impatto sui nostri clienti abbiamo attivato le seguenti azioni:

- [*Elenca le azioni intraprese dalla tua organizzazione per garantire che questa violazione non venga ripetuta, ancora una volta non è necessario compromettere la riservatezza dell'organizzazione, ma occorre rassicurare l'interessato.*]

Nota: non invieremo ulteriori aggiornamenti via e-mail su questo incidente. Tutti gli aggiornamenti futuri in merito a questa violazione della sicurezza possono essere consultati sul nostro sito web all'indirizzo: [www.asp.enna.it]. Qualsiasi e-mail dovreste ricevere su questo incidente di sicurezza deve essere considerata sospetta.
Ci scusiamo con tutto il cuore per questa violazione della sicurezza, ma le assicuriamo che stiamo facendo tutto ciò che è in nostro potere per garantire che il danno sia mitigato e che ciò non accada di nuovo in il futuro. Per ulteriori informazioni si prega di contattare [----------]

Cordiali Saluti.

[*Nome e cognome*]

REGIONE SICILIANA
AZIENDA SANITARIA PROVINCIALE
ENNA

Codice fiscale / P. IVA 01151150867

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

(ai sensi del REGOLAMENTO (UE) n. 679/2016 e del D. Lgs. n. 101/2018)

CONSENSO AL TRATTAMENTO DEI DATI

Gentile utente,

questo documento Le fornisce tutte le informazioni ex artt. 13 e 14 del Regolamento UE 679/2016, di cui potrà prendere visione sul sito del Garante per la Protezione dei Dati Personali *(http://www.garanteprivacy.it/regolamentoue)*,

La informiamo che i dati personali che La riguardano saranno trattati ed utilizzati dai dipendenti di questa Azienda Sanitaria, ai sensi del GDPR Privacy e del D.Lgs n. 101/2018, nel rispetto della riservatezza, del segreto professionale, del segreto d'ufficio, dei diritti e delle libertà fondamentali della persona, della dignità individuale.

Il trattamento dei dati personali sarà improntato ai principi di legittimità, correttezza, liceità, indispensabilità, pertinenza e non eccedenza rispetto agli scopi per i quali i dati medesimi sono stati raccolti.

TITOLARE DEL TRATTAMENTO

Titolare del trattamento è l'Azienda Sanitaria Provinciale di Enna, con sede legale in Enna in viale A. Diaz n. 7/9, Centralino 0935-516111, Codice Fiscale/Partita IVA 01151150867, PEC: protocollo.generale@pec.asp.enna.it, sito web: www.asp.enna.it.

Rappresentante legale: Dr. Antonino Salina, Commissario straordinario; e-mail: direzione.generale@asp.enna.it

Responsabile della protezione dei dati (DPO): Dr. Angelo Di Pasquale, e-mail: privacy@asp.enna.it, PEC: ced@pec.asp.enna.it.

Responsabile del trattamento: Il Responsabile del trattamento dei dati, relativamente alle attività demandate alla competenza di ciascuna Unità Operativa è il Direttore U.O.C. di riferimento. L'elenco dei Responsabili è consultabile sul sito web aziendale.

Conformemente all'art. 28 del GDPR, il Responsabile del trattamento mette in atto le misure tecniche ed organizzative adeguate, in modo tale che il trattamento dei dati personali si esplichi in ottemperanza al GDPR e garantisca la tutela dei diritti dei soggetti interessati.

DEFINIZIONE DI DATI E CATEGORIE

Per dati si intendono le informazioni inerenti alle persone fisiche (utenti, fornitori, pazienti, dipendenti, utilizzatori di farmaci e dispositivi, convenzionati).

Ai sensi degli artt. 9 e 10 del Reg. UE n. 679/2016, il trattamento concerne le seguenti categorie di dati:

DATI IDENTIFICATIVI

- comuni e anagrafici (a titolo esemplificativo: nome, cognome, ragione sociale, indirizzo, e-mail, codice fiscale);

PARTICOLARI CATEGORIE DI DATI PERSONALI:

- dati genetici e biometrici (intesi a identificare in modo univoco una persona fisica);
- dati sensibili, informazioni sullo stato di salute, origine razziale o etnica, convinzioni religiose, politiche o filosofiche, appartenenza sindacale, vita o orientamento sessuale,
- dati giudiziari idonei a rivelare le risultanze del casellario giudiziale, sanzioni, imputazioni, indagini di reato.

Tali categorie di dati potranno essere trattati dall'ASP di Enna solo previo Suo esplicito consenso, manifestato in forma scritta.

FINALITA' DEL TRATTAMENTO E BASE GIURIDICA

I dati personali saranno trattati ed utilizzati, ai sensi dell'art. 9 - punto h) del Regolamento n. 679/2016, per finalità connesse e strumentali alla tutela della salute e per lo svolgimento delle seguenti attività (elencate a titolo esemplificativo):

- salvaguardia di interessi vitali e incolumità fisica;
- prevenzione, diagnosi e cura;
- tutela socio-assistenziale e interventi di rilievo sanitario;
- adempimento di obblighi legali;
- operazioni contrattuali, precontrattuali e di esecuzione del contratto;
- adempimenti amministrativi, gestionali e contabili;
- certificazioni relative allo stato di salute;
- ricerca scientifica e statistica;
- attività di programmazione, gestione, controllo, statistica e valutazione sanitaria;
- finalità formative (personale non strutturato (specializzandi, volontari o tirocinanti)
- compiti di interesse pubblico o connessi all'esercizio di pubblici poteri,
- gestione della documentazione sanitaria e clinica, anche in formato elettronico.

La base giuridica è rappresentata: dal consenso dell'interessato al trattamento dei dati comuni e sensibili, raccolti e trattati per specifiche finalità; dalla salvaguardia degli interessi vitali dell'interessato, dal GDPR 2016/679, dal D. Lgs. 196/203 "Codice in materia di protezione dei dati personali", Leggi nazionali e regionali in materia di Sanità pubblica.
La comunicazione dei dati personali è un requisito necessario e la mancata comunicazione o il mancato consenso rendono impossibile l'esecuzione della prestazione da parte dell'ASP di Enna, fatta eccezione per le prestazioni urgenti disposte per legge.
Il trattamento si basa su un legittimo interesse e sulla necessità di adempiere ad un obbligo legale a cui è soggetta l'A.S.P. di Enna.

CONSENSO DELL'INTERESSATO

Il consenso al trattamento dei dati, acquisito da operatori autorizzati, è indispensabile per poter usufruire delle prestazioni richieste e/o necessarie per la tutela della salute, sia in regime di degenza, sia in regime ambulatoriale.
Il mancato consenso al trattamento dei dati, con l'eccezione dei trattamenti urgenti e di quelli disposti da una pubblica autorità (Sindaco, Magistrato), comporta l'impossibilità di erogare la prestazione richiesta.
Il consenso al trattamento le sarà chiesto al primo accesso e resterà valido, salvo che Lei non decida di revocarlo.
L'espressione del consenso potrà essere esercitata mediante compilazione del "Modulo di consenso" allegato alla presente informativa.

MODALITA' DI TRATTAMENTO

I trattamenti potranno essere effettuati mediante strumenti informatici e cartacei, con modalità audio e video, telefono, e fax, nell'osservanza di tutte le cautele necessarie a garantire la sicurezza e la riservatezza delle informazioni, adottando misure tecniche ed organizzative atte a scongiurare trattamenti non autorizzati o illeciti, la loro perdita o distruzione.
Verranno assicurate le adeguate garanzie che possono comprendere la cifratura o la pseudonimizzazione.
I dati potranno essere trattati, se necessario nell'ambito della teleassistenza/telemedicina, anche tramite collegamento telematico bidirezionale con altre strutture, si potrà adottare un processo decisionale automatizzato, compresa la profilazione.
I dati personali e sensibili saranno comunque protetti, in modo da garantire la sicurezza, la riservatezza e l'accesso al solo personale autorizzato.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

I dati potranno essere trattati dai dipendenti dell'A.S.P. nell'espletamento delle funzioni aziendali deputate al perseguimento delle finalità proprie, autorizzati al trattamento, a seguito di adeguate istruzioni operative.

PERIODO DI CONSERVAZIONE

La conservazione dei dati avverrà secondo specifici criteri dettati dalla legge e/o da regolamenti.
Potrà prendere visione in maniera dettagliata dei tempi di conservazione inerenti tutte le attività, i documenti, gli atti ed i certificati consultando il massimario pubblicato sul sito web dell'Azienda Sanitaria di Enna, link: privacy.
Si elencano una serie di casi, a mero titolo esemplificativo:
- documenti contabili: 10 anni;
- cartelle cliniche, unitamente ai relativi referti ed esami clinici, e referti operatori: illimitatamente;
- turni del personale e giustificativi assenze, cedolini paga: 10 anni;
- contenzioso giudiziale: fino all'esaurimento dei termini di esperibilità delle azioni di impugnazione;

Il Titolare provvede all'eliminazione di ogni dato trattato con cadenza periodica regolare e con modalità idonee a non pregiudicare la privacy.

DIRITTI DELL'INTERESSATO

Lei ha diritto di esercitare, ai sensi degli artt. 15-21 del regolamento UE, in qualsiasi momento:
- l'accesso ai dati che La riguardano;
- la richiesta di informazioni sulle finalità del trattamento e sull'utilizzo dei dati;
- la rettifica;
- la cancellazione in tutto o in parte ("diritto all'oblio"), purché non sussistano obblighi di conservazione per legge;
- la limitazione del trattamento nelle ipotesi previste dall'art. 18 GDPR;
- la facoltà di proporre reclamo ad un'Autorità di controllo, ai sensi dell'art. 77 del regolamento UE n. 679/2016, o di adire le opportune sedi giudiziarie (art. 79 Reg. UE 679/2016);
- la richiesta delle informazioni disponibili sull'origine dei dati, qualora gli stessi non siano raccolti presso l'interessato;
- l'informazione sull'esistenza di un processo decisionale automatizzato, compresa la profilazione;
- la facoltà di opporsi al trattamento;
- la trasmissione ad altro titolare (cd. "diritto alla portabilità);
- la facoltà di opporsi ad un processo decisionale automatizzato, compresa la profilazione;
- la possibilità di rivolgere una segnalazione al Garante privacy, ex art. 13 del D. Lgs n. 101/2018;

La richiesta di rettifica, cancellazione, limitazione e revoca del consenso non pregiudicano la liceità del trattamento basata sul consenso prestato in precedenza.

DIRITTO DI REVOCA DEL CONSENSO

Lei ha il diritto di revocare in ogni momento, ex art. 7.3 GDPR, il consenso al trattamento dei dati.
La revoca non pregiudica la liceità del trattamento basata sul consenso prima della revoca.
Tale diritto potrà essere esercitato mediante compilazione del modulo di consenso allegato alla presente informativa.

MODALITA' DI ESERCIZIO DEI DIRITTI

I diritti dell'interessato possono essere esercitati con apposita istanza inviata al titolare del trattamento da presentare al protocollo di questa A.S.P. di Enna o da inoltrare via PEC, raccomandata postale o e-mail.
Gli Uffici URP saranno a Sua disposizione per ogni informazione.

COMUNICAZIONE E TRASFERIMENTO DEI DATI

I dati personali non saranno soggetti a diffusione (non possono essere resi noti ad un numero indistinto di soggetti) e non saranno oggetto di trasferimento all'estero.
I dati possono essere comunicati a soggetti esterni, operanti in qualità di titolari del trattamento, per il raggiungimento di particolari finalità e nei casi previsti da norme di legge e di regolamento.
A titolo esemplificativo si riportano alcuni soggetti ai quali l'A.S.P. di Enna potrà comunicare i dati:
- autorità, organi di vigilanza e controllo, istituzioni pubbliche;
- soggetti pubblici o privati ed altre Aziende Sanitarie, coinvolti nel percorso diagnostico-terapeutico;
- Regione (per attività amministrative di competenza regionale);
- Azienda sanitaria di residenza (se diversa da quella di accesso);
- Comune di residenza;
- Servizi sociali (per attività connesse all'assistenza dei soggetti deboli);
- Forze dell'ordine e Autorità giudiziaria;
- Soggetti qualificati ad intervenire in controversie in cui è parte l'Azienda (compagnia assicurativa, ecc..);
- Medici di medicina generale e pediatri di libera scelta;
-INPS e INAIL.

I dati potranno essere trattati, per conto del titolare, da soggetti esterni designati come Responsabili del trattamento, che svolgono specifiche attività (a titolo esemplificativo: adempimenti contabili, fiscali e assicurativi, spedizione e corrispondenza, gestione incassi e pagamenti, ecc...).
I dati potranno essere conosciuti dai collaboratori del titolare, specificamente autorizzati in qualità di Responsabili incaricati dell'espletamento di specifiche funzioni e competenze.

PRESA VISIONE DELL'INFORMATIVA

Io sottoscritto:
Nome _____ Cognome _____ nato a _____ il _____
residente in _____ Via _____ n. __ C.F. _____
documento di riconoscimento _____
in qualità di diretto interessato o esercente la potestà genitoriale/la tutela/la curatela/l'amministrazione di sostegno su
Nome _____ Cognome _____ nato a _____ il _____
C.F. _____ residente in _____ Via _____ n. __
dichiaro di aver preso visione della presente informativa.

DATA _____ FIRMA _____

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

(art. 7 Reg. UE n. 679/2016 e D. Lgs. n. 101/2018)

Io sottoscritto:
Nome _____ Cognome _____ nato a _____ il _____
residente in _____ Via _____ n. __ C.F. _____
Documento di riconoscimento _____

in qualità di diretto interessato o esercente la potestà genitoriale/la tutela/la curatela/l'amministrazione di sostegno su

Nome _____ Cognome _____ nato a _____ il _____
C.F. _____ residente in _____ Via _____ n. __

- o esprimo il consenso al trattamento dei miei dati personali;
- o non esprimo il consenso al trattamento dei miei dati personali;

- o esprimo il consenso alla comunicazione dei miei dati ad altri soggetti, secondo quanto indicato nella presente informativa
- o non esprimo il consenso alla comunicazione dei mie dati ad altri soggetti, secondo quanto indicato nella presente informativa

- o esprimo il consenso al trattamento delle categorie particolari dei miei dati personali
- o non esprimo il consenso al trattamento delle categorie particolari dei miei dati personali

- o esprimo il consenso al trattamento delle seguenti categorie particolari dei miei dati personali _____
- o non esprimo il consenso al trattamento delle seguenti categorie particolari dei miei dati personali _____

- nel caso di esercenti la potestà:
  il genitore presente dichiara che l'altro genitore esercente la potestà sul minore è informato e acconsente al trattamento dei dati personali.
- nel caso di impossibilità dell'interessato a prestare il consenso per incapacità, anche temporanea:
  il soggetto che autorizza il trattamento dati (familiare, convivente, responsabile di struttura) si impegna, non appena l'interessato sia in grado di prestare autonomamente il consenso, a comunicargli di averlo prestato in sua vece e della possibilità di revocarlo.

DATA _____ FIRMA _____ *

*(Possono sottoscrivere i soggetti di età maggiore di anni 14 ex D. Lgs. n. 101/2018)

Azienda Sanitaria Provinciale di Enna
Viale Diaz n.7/9 94100 Enna
C. F. e P.IVA 01151150867

DESIGNAZIONE INCARICATI TRATTAMENTO DEI DATI PERSONALI (REG. UE 679/2016, D. Lgs. n. 101/2018, D. Lgs. n. 196/2003)

Al dipendente_____
Ufficio/Servizio _____

Oggetto: Atto di designazione a incaricato del trattamento dati personali nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n. 679/2016 – Atto di designazione dei dipendenti/delle persone fisiche preposte alla UOC/UOS, che operano sotto la diretta autorità del responsabile, per il trattamento dei dati personali, e conseguente attribuzione di specifici compiti e funzioni, con delega all'esercizio e allo svolgimento degli stessi secondo analitiche istruzioni impartite.

IL DIRIGENTE/RESPONSABILE U.O.C. _____

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo GDPR);

Rilevato che il suddetto GDPR risulta immediatamente operativo, in tutti gli Stati membri, a decorrere dal 25 maggio 2018;

Vista la legge 25 ottobre 2017, n. 163, recante "*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017*" e, in particolare, l'art. 13, che delega il Governo all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;

Visto il D.Lgs. 101/2018 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Visto il decreto legislativo attuativo della delega, e recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR;

Rilevato che, ai fini dell'adeguamento, vanno innanzitutto individuati gli attori, i ruoli e le responsabilità del sistema di sicurezza preordinato a garantire la protezione dei dati personali;

Considerato che l'attuale assetto dei soggetti e delle responsabilità connesse al trattamento dei dati risulta basato sulla disciplina del D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (di

seguito semplicemente "Codice"), nel testo previgente all'adeguamento al GDPR;

Tenuto presente che la disciplina degli incaricati al trattamento dei dati, contenuta nell'art. 30 del D.Lgs. n. 196/2003, nel testo previgente all'adeguamento al GDPR, prevedeva che *"1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. 2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima"*;

Dato atto che il GDPR non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'articolo 29, rubricato *"Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento"*, il quale stabilisce che *"il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"*;

Rilevato che dalla suddetta disposizione si evince la permanenza del ruolo degli incaricati, da intendersi come persone fisiche che agiscono sotto l'autorità del titolare o del responsabile del trattamento;

Dato atto che il GDPR e la normativa nazionale di adeguamento, consentono di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione;

Considerato che, conformemente alle disposizioni del GDPR, e della normativa interna di adeguamento, il titolare o il responsabile del trattamento possono quindi designare, sotto la propria responsabilità, e all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati;

Ritenuto che le modalità più opportune siano costituite dalla delega di specifici compiti e funzioni alle persone fisiche designate;

Dato atto che si rende necessario procedere alla designazione delle persone fisiche aventi specifici compiti e funzioni connessi al trattamento dei dati personali, e alla delega dell'esercizio e dello svolgimento di tali specifici compiti e funzioni alle persone fisiche designate;

Richiamata la delibera _____ e l'atto di nomina prot. n. _____ del _____ con i quali il titolare del trattamento ha attribuito al sottoscritto dirigente/responsabile UOC specifici compiti e funzioni connesse al trattamento dei dati personali;

Dato atto che, tra le competenze del responsabile del trattamento sono espressamente ricompresi anche il compito e la funzione di identificare e designare, per iscritto e in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura di competenza, le persone fisiche della struttura medesima, che operano sotto la diretta autorità del titolare/responsabile, e di attribuire alle persone medesime specifici compiti inerenti al trattamento dei dati inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni, e controllando costantemente che le persone fisiche designate e delegate al trattamento dei dati effettuino le operazioni di trattamento:

- in attuazione del principio di «liceità, correttezza e trasparenza»;
- in attuazione del principio di «minimizzazione dei dati»;
- in attuazione del principio di «limitazione della finalità»;
- in attuazione del principio di «esattezza»;
- in attuazione del principio di «limitazione della conservazione»;
- in attuazione del principio di «integrità e riservatezza»;

Considerato l'organigramma funzionale degli Uffici e dei servizi;

Dato atto che nel:
Settore/UOC/Servizio _____
Ufficio _____
Sede _____
è preposto il dipendente sotto elencato:

NOME E COGNOME	RUOLO FUNZIONI COMPETENZE
QUALIFICA _____	

- Rilevato che il dipendente sopra menzionato:
  - gestisce, per quanto rientra nelle proprie funzioni, i processi/procedimenti dell'Ufficio;
  - effettua, in forza di atto di nomina ad incaricato, in atti, il trattamento dei dati personali, sensibili e giudiziari di tutti i processi/procedimenti e di tutti i soggetti con i quali il titolare si relaziona nell'ambito della sua attività istituzionale connessa a tutti i processi/procedimenti dell'Ufficio;
- Vista la ricognizione dei trattamenti dei dati personali in correlazione ai processi/procedimenti dell'Ufficio;
- Tenuta presente la valutazione di impatto sulla protezione dei dati per i trattamenti che possono presentare un rischio elevato (DPIA);
- Considerato che il contenuto dell'atto di nomina a incaricato deve essere conforme alle misure finalizzate a dare attuazione alle disposizioni del GDPR;
- Ferma restando la Responsabilità in capo al Dirigente designato dal titolare del trattamento dati;
- Visto il Regolamento per la tutela ed il trattamento dei dati personali dell'A.S.P. di Enna, pubblicato sul sito web – area: Privacy;

DESIGNA

- con decorrenza dalla data di ricezione del presente provvedimento, _____ (nome e cognome), che opera sotto la diretta autorità del Responsabile, quale persona fisica a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali, relativi ai trattamenti rientranti nella struttura organizzativa di competenza, e di seguito elencati, dando atto che i compiti e funzioni attribuite devono essere svolti:

- - presso la sede _____ in Via _____ n. _____ , _____;
- - nell'ambito e conformemente alle istruzioni contenute nel presente atto di designazione

TRATTAMENTI

rientranti nella struttura organizzativa di competenza		
Ufficio	**Denominazione trattamento**	**Operazioni trattamento eseguibili**

A seguito e per l'effetto della presente designazione, il sottoscritto dirigente/responsabile di UOC:

ATTRIBUISCE

- con decorrenza dalla data di sottoscrizione del presente atto, a _____ (nome e cognome), che opera sotto la diretta autorità del titolare/responsabile, i compiti e le funzioni analiticamente elencate in calce la presente atto, con facoltà di successiva integrazione e/o modificazione, dando atto che l'attribuzione di compiti e funzioni inerenti il trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita ma conferisce soltanto il potere/dovere di svolgere i compiti e le funzioni attribuite dal titolare;

DELEGA

- con decorrenza dalla data di sottoscrizione del presente atto, _____ (nome e cognome), che opera sotto la diretta autorità del titolare, il compito di trattare i dati personali inclusi nell'elenco dei trattamenti in precedenza indicati, conferendo formale potere e autorizzazione di compiere, secondo le specifiche istruzioni e prescrizioni sotto indicate, tutte le operazioni di trattamento di dati personali attinenti alla funzione rivestita.

La presente designazione e delega:

- costituisce formale autorizzazione a trattare dati personali conformemente al GDPR, alla normativa interna di adeguamento, alle Linee guida delle Autorità di controllo, alle specifiche istruzioni sulle modalità a cui attenersi nel trattamento di seguito indicate e, infine, alle eventuali indicazioni del RPD/DPO;
- ha validità per l'intera durata del rapporto di lavoro;
- viene a cessare al modificarsi del rapporto di lavoro o con esplicita revoca.

DISPONE

- la notificazione a mezzo_____ o, in alternativa, la comunicazione personale, con rilascio di apposita dichiarazione di ricevimento dell'atto soprascritto.

4

Azienda Sanitaria Provinciale di Enna
Viale Diaz n.7/9 94100 Enna
C. F. e P.IVA 01151150867

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI VADEMECUM E SPECIFICHE ISTRUZIONI AI SOGGETTI DESIGNATI

Il titolare del trattamento, per il tramite del sottoscritto dirigente UOC designato Responsabile del trattamento dei dati, ed in forza del principio di «responsabilizzazione», impartisce alla persona fisica designata e delegata al trattamento, e sopra indicata, le istruzioni a cui è obbligata ad attenersi.

Cosa sono i dati personali

Il Codice definisce dato personale "*qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*".

I dati personali possono essere:

- comuni: tutti i dati che non appartengono ai dati sensibili o alle informazioni di carattere giudiziario
- ☐ sensibili
- ☐ giudiziari.

Si sottolinea l'importanza di comprendere quando un dato è considerato sensibile e/o a carattere giudiziario: a questi dati è infatti garantita una tutela più intensa, per cui sono imposti maggiori obblighi ed oneri nell'effettuare il trattamento e nella loro custodia.

1) I dati sensibili

Sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

2) I dati giudiziari

Sono i dati personali idonei a rivelare i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. n. 313 del 14/11/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.

3) Implicazioni operative

Nella lettera di nomina di ciascun Incaricato sono indicati i dati sensibili e/o a carattere giudiziario che l'Incaricato è autorizzato a trattare, in relazione allo svolgimento delle sue mansioni. Qualora, nello svolgimento della sua attività lavorativa, dovesse venire in possesso di informazioni, sensibili o di carattere giudiziario, che esulano da tale autorizzazione, l'Incaricato è invitato a rivolgersi al Responsabile dei Trattamenti della propria Struttura di appartenenza, per ricevere le istruzioni del caso.

Cosa è il trattamento dei dati personali

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

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 sono assoggettati alla normativa Privacy.

Le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

1. il reperimento delle informazioni

2. il trattamento "interno" delle informazioni
3. l'uso delle informazioni nei rapporti con l'esterno.

b1) Il reperimento delle informazioni

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

b2) Il trattamento interno delle informazioni

Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti
- la organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera
- la elaborazione, ovvero le operazioni che attribuiscono significatività ai dati, in relazione allo scopo per il quale essi sono stati raccolti
- la consultazione di dati che siano stati in precedenza registrati, organizzati ed elaborati
- la selezione, la estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni
- la interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto
- il blocco, ovvero la conservazione dei dati con sospensione temporanea di ogni altra operazione di trattamento
- la conservazione dei dati, alla quale il codice dedica particolari attenzioni sotto il profilo della sicurezza
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

b3) L'uso delle informazioni nei rapporti con l'esterno

Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della privacy altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni.

L'utilizzo può essere:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni
- ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo cui il Codice dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:

- la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
- la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

3

b4) Implicazioni operative

Nella lettera di incarico potrà essere posto particolare accento sui dati che l'Incaricato è autorizzato a comunicare a terzi, esterni all'Azienda, e/o a diffondere, in relazione allo svolgimento delle sue mansioni. Qualora ciascun Incaricato, nello svolgimento della sua attività lavorativa, si trovasse nella situazione di dovere procedere ad una comunicazione o diffusione di dati, oltre i limiti previsti in tale autorizzazione, è invitato a rivolgersi al Responsabile dei Trattamenti della propria Struttura di appartenenza, per ricevere le istruzioni del caso.

c) Prescrizioni generali su come deve avvenire il trattamento dei dati

I dati personali oggetto di trattamento devono essere:

a) trattati in modo lecito e secondo correttezza

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, ed in ogni caso nei limiti in cui il

trattamento sia necessario per il funzionamento dell'Azienda
c) esatti e, se necessario, aggiornati
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati
e) conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
Sarà cura dell'Incaricato 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 correttezza, si richiama l'attenzione dell'Incaricato sulla necessità di dare prontamente soddisfazione alle richieste che i soggetti interessati possono inoltrare, conformemente a quanto prescritto dall'articolo 7 del D.Lgs. n. 196/2003 (Diritto di accesso ai dati personali ed altri diritti), segnalando inoltre tali richieste al Responsabile al Responsabile dei Trattamenti della propria Struttura di appartenenza, qualora il loro soddisfacimento esuli dai propri compiti.

Descrizione degli incarichi

In relazione alle mansioni lavorative affidate, all'Incaricato viene dato l'incarico di trattare i seguenti dati personali *:*

☐ dati di natura comune, 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

☐ dati di natura sensibile e/o giudiziaria 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

☐ dati di natura comune, che consistono in informazioni di carattere anagrafico ed in altre notizie il cui trattamento è necessario in relazione allo svolgimento dell'attività lavorativa, di fornitori. Tali dati non potranno essere comunicati al di fuori dell'Azienda

☐ dati che si riferiscono al personale dell'Azienda, sia comuni che di natura sensibile: con riferimento a questi ultimi, l'Incaricato 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.

Le misure fisiche di custodia dei dati

I dati di natura comune, necessari per lo svolgimento delle mansioni lavorative, sono, di norma, custoditi nell'archivio, costituito dagli scaffali posti nei locali adibiti ad area lavorativa. Taluni archivi potranno essere ad accesso selezionato, per cui l'Incaricato può accedervi nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti ed i supporti informativi, necessari per lo svolgimento delle sue mansioni lavorative. Durante i periodi di temporanea assenza dell'Incaricato ed al termine della sua giornata lavorativa, tali documenti dovranno essere riposti, nei cassetti di cui è dotata la scrivania. Una volta terminato il lavoro, per svolgere il quale si è reso necessario utilizzare i documenti, essi dovranno essere restituiti all'archivio.

4

I dati di natura sensibile, necessari per lo svolgimento delle mansioni lavorative, sono custoditi nell'archivio costituito dall'armadio, munito di serratura. Tali archivi potranno essere ad accesso controllato, per cui l'Incaricato può accedervi solo previa richiesta della chiave al Responsabile dei Trattamenti della propria Struttura di appartenenza, che durante l'orario lavorativo detiene la chiave stessa.
Qualora avesse necessità di accedere a tale archivio dopo l'orario lavorativo, l'Incaricato 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.

I documenti contenenti informazioni di carattere sensibile dovranno essere riposti dall'Incaricato, durante i periodi di temporanea assenza ed al termine della giornata lavorativa, nei cassetti con serratura di cui è dotata la sua scrivania, avendo cura di chiudere gli stessi a chiave.

Una volta terminato il lavoro, per svolgere il quale si è reso necessario utilizzare tali documenti, essi dovranno essere restituiti all'archivio.

L'attribuzione di dispositivi e codici per accedere ai Personal Computer ed ai dati contenuti

Nello svolgimento dei suoi compiti, l'Incaricato potrà essere autorizzato ad accedere al Personal Computer a lui reso disponibile dall'Azienda, previa verifica della sua identità. A tale fine:

□ all'Incaricato viene fornito, dall'Amministratore del sistema, un codice di identificazione (*username*), che dovrà provvedere a mantenere segreto. Qualora avesse il sospetto che terzi siano venuti a conoscenza dello stesso, dovrà informarne immediatamente il Responsabile dei Trattamenti della propria Struttura di appartenenza.

□ gli viene fornita una parola chiave (*password*), composta di almeno otto caratteri alfanumerici, che dovrà provvedere a modificare in occasione del primo accesso al P.C., e successivamente almeno ogni sei mesi, nèl caso in cui tratti solo dati di natura comune, o almeno ogni tre mesi, nel caso in cui tratti anche dati di natura sensibile o giudiziaria.

Si raccomanda di fare uso di caratteri sia alfabetici che numerici, che formino un codice non banale o facilmente individuabile.

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 di appartenenza, o ad altro soggetto da questi delegato.

Il reimpiego dei supporti di memorizzazione

Al termine dell'utilizzo dei dischetti, e degli altri supporti di memorizzazione contenenti dati sensibili e/o di natura giudiziaria, questi dovranno essere consegnati al proprio diretto superiore gerarchico, che adotterà le procedure necessarie per cancellare ogni informazione contenuta in tali dischetti, prima di autorizzarne il reimpiego.

L'utilizzo dei software di protezione

Si raccomanda di utilizzare i software di protezione di cui dispone l'Azienda, le cui specifiche tecniche verranno fornite all'Incaricato, oltre che in questa sede, ogni volta che vi sono dei significativi aggiornamenti. Si sottolinea, in particolare, l'importanza di controllare metodicamente tutti i files (archivi elettronici) provenienti dall'esterno e di adottare diligentemente le opportune cautele, al momento della trasmissione all'esterno di files dell'Azienda.

L'utilizzo della posta elettronica

Per lo svolgimento delle mansioni lavorative, all'Incaricato potrà essere 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 dell'Incaricato.

L'utilizzo di Internet

Ad alcuni Incaricati, appositamente individuati dal diretto superiore gerarchico, verrà attribuito l'accesso ad Internet, del quale è consentito usufruire solo nei limiti strettamente necessari per lo svolgimento dell'attività lavorativa.

Si rammenta che è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore.

Prima di procedere allo scarico di qualsiasi file o programma, anche a titolo gratuito, dovrà inoltre chiedere l'autorizzazione al diretto superiore gerarchico.

Prescrizione residuale

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati personali, l'Incaricato può rivolgersi al Responsabile dei Trattamenti della propria Struttura di appartenenza, per ricevere le dovute istruzioni.

In particolare, nella gestione dei processi/procedimenti dell'Ufficio a cui la persona fisica designata al trattamento è preposta e, più in generale, nello svolgimento dell'attività lavorativa presso detto Ufficio, la delega ad effettuare le operazioni di trattamento dei dati personali nell'ambito della suddetta attività, viene rilasciata con le seguenti istruzioni che costituiscono cogenti prescrizioni, anche ai fini della responsabilità personale:

4

- in attuazione del principio di «liceità, correttezza e trasparenza», raccolta, registrazione, elaborazione di dati, agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nell'Ufficio di appartenenza, nell'osservanza delle tecniche e metodologie in atto;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui la persona fisica designata e delegata al trattamento è preposta;
- in attuazione del principio di «limitazione della finalità» trattamento conforme alle finalità istituzionali del titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, e obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione», obbligo di conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nell'Ufficio di competenza, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti dati sensibili vengano conservati in contenitori/armadi muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente e integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- in attuazione del principio di «liceità, correttezza e trasparenza», autorizzazione a comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal titolare del trattamento.

• Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.

In particolare, per tali trattamenti la persona fisica designata e delegata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

-Password e username (credenziali di autenticazione informatica)

1) Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise con altri incaricati del trattamento. La password che la persona fisica designata e delegata al trattamento imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'amministratore del sistema, del custode delle parole chiave o del Dirigente dell'Ufficio,

2) Non deve essere riconducibile alla persona designata;

3) deve essere cambiata almeno ogni 3 mesi dal designato medesimo.

- **Logout**

  La persona fisica designata e delegata al trattamento, al termine di ogni sessione di trattamento ha l'obbligo di uscire dall'applicazione utilizzata e di effettuare il logout.

- **Supporti di tipo magnetico e/o ottico**

  La persona fisica designata e delegata al trattamento, ha l'obbligo di:

  - proteggere i dati personali archiviati su supporti di tipo magnetico e/o ottico con le stesse misure di sicurezza previste per i supporti cartacei;

- verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione;
- di rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al sottoscritto dirigente UOC.

Data _____

Il Dirigente/Responsabile UOC

_____

Dichiarazione di ricevimento dell'atto di designazione, autorizzazione e delega soprascritto e di impegno all'osservanza delle istruzioni

Il/La sottoscritto/a _____

Dichiara

1. di aver ricevuto il sovrascritto atto di designazione, attribuzione e delega al trattamento dei dati personali;
2. di aver attentamente letto e compreso il contenuto di detto atto, e di impegnarsi a osservare tutte le specifiche istruzioni impartite;
3. di obbligarsi a rispettare i divieto di comunicazione e diffusione dei dati trattati;
4. di dare atto che l'obbligo di riservatezza, correlato all'incarico, va osservato anche per il tempo successivo alla sua cessazione della designazione medesima.

Data _____

Il dipendente designato

_____

6

Azienda Sanitaria Provinciale di Enna
Viale Diaz n.7/9 94100 Enna
C. F. e P.IVA 01151150867

VADEMECUM PER GLI INCARICATI DEI TRATTAMENTI

Cosa sono i dati personali

Il dato personale è qualsiasi informazione relativa a persona fisica, persona giuridica, ente od associazione, identificata o identificabile, anche indirettamente, mediante riferimento a un identificativo come il nome ed elementi caratteristici della sua identità fisica, genetica, economica, culturale, sociale.

I dati personali possono essere:

- comuni: tutti i dati che non appartengono ai dati sensibili o alle informazioni di carattere giudiziario (es. indirizzo, codice fiscale, e-mail)
- sensibili
- giudiziari

Si sottolinea l'importanza di comprendere quando un dato è considerato sensibile e/o a carattere giudiziario: a questi dati è infatti garantita una tutela più intensa, per cui sono imposti maggiori obblighi ed oneri nell'effettuare il trattamento e nella loro custodia.

1) I dati sensibili

Sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

2) I dati giudiziari

Sono i dati personali idonei a rivelare i provvedimenti di cui all'articolo 3, comma 1, lettere da a) o) e da r) a u), del D.P.R. n. 313 del 14/11/2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.

Cosa è il trattamento dei dati personali

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

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 sono assoggettati alla normativa Privacy.

Le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

1. il reperimento delle informazioni
2. il trattamento "interno" delle informazioni
3. l'uso delle informazioni nei rapporti con l'esterno.

1) Il reperimento delle informazioni

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

Nell'ambito di tale fase assume una preminente importanza la sottoscrizione del modulo di "Informativa" e di "Consenso informato".

2) Il trattamento interno delle informazioni

Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

☐ la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti

☐ la organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera

☐ la elaborazione, ovvero le operazioni che attribuiscono significatività ai dati, in relazione allo scopo per il quale essi sono stati raccolti

☐ la consultazione di dati che siano stati in precedenza registrati, organizzati ed elaborati

☐ la selezione, la estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione

☐ la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni

☐ la interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto

☐ il blocco, ovvero la conservazione dei dati con sospensione temporanea di ogni altra operazione di trattamento

☐ la conservazione dei dati, alla quale il codice dedica particolari attenzioni sotto il profilo della sicurezza

☐ la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

3) L'uso delle informazioni nei rapporti con l'esterno

Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della privacy altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni.

L'utilizzo può essere:

• diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni

• ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Tali operazioni sono potenzialmente lesive della privacy, trattandosi di quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:

☐ la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione

☐ la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Implicazioni operative

Nella lettera di incarico potrà essere posto particolare accento sui dati che l'Incaricato è autorizzato a comunicare a terzi, esterni all'Azienda, e/o a diffondere, in relazione allo svolgimento delle sue mansioni. Qualora ciascun Incaricato, nello svolgimento della sua attività lavorativa, si trovasse nella situazione di dovere procedere ad una comunicazione o diffusione di dati, oltre i limiti previsti in tale autorizzazione, è invitato a rivolgersi al Responsabile dei Trattamenti della propria Struttura di appartenenza, per ricevere le istruzioni del caso.

Prescrizioni generali su come deve avvenire il trattamento dei dati

I dati personali oggetto di trattamento devono essere:

a) trattati in modo lecito e secondo correttezza

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi, ed in ogni caso nei limiti in cui il trattamento sia necessario per il funzionamento dell'Azienda

c) esatti e, se necessario, aggiornati

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati

e) conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Sarà cura dell'Incaricato 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 correttezza, si richiama l'attenzione dell'Incaricato sulla necessità di dare prontamente soddisfazione alle richieste che i soggetti interessati possono inoltrare, conformemente a quanto prescritto
dal Regolamento Aziendale sul Diritto di accesso. Segnalando inoltre tali richieste al Responsabile al Responsabile dei Trattamenti della propria Struttura di appartenenza, qualora il loro soddisfacimento esuli dai propri compiti.

Descrizione degli incarichi

In relazione alle mansioni lavorative affidate, all'Incaricato viene dato l'incarico di trattare i seguenti dati personali:

☐ dati di natura comune, 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

☐ dati di natura sensibile e/o giudiziaria 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

☐ dati di natura comune, che consistono in informazioni di carattere anagrafico ed in altre notizie il cui trattamento è necessario in relazione allo svolgimento dell'attività lavorativa. Tali dati non potranno essere comunicati al di fuori dell'Azienda

☐ dati che si riferiscono al personale dell'Azienda, sia comuni che di natura sensibile: con riferimento a questi ultimi, l'Incaricato 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.

Le misure fisiche di custodia dei dati

I dati di natura comune, necessari per lo svolgimento delle mansioni lavorative, sono, di norma, custoditi nell'archivio, costituito dagli scaffali posti nei locali adibiti ad area lavorativa. Taluni archivi potranno essere ad accesso selezionato, per cui l'Incaricato può accedervi nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti ed i supporti informativi, necessari per lo svolgimento delle sue mansioni lavorative. Durante i periodi di temporanea assenza dell'Incaricato ed al termine della sua giornata lavorativa, tali documenti dovranno essere riposti, nei cassetti di cui è dotata la scrivania. Una volta terminato il lavoro, per svolgere il quale si è reso necessario utilizzare i documenti, essi dovranno essere restituiti all'archivio.

I dati di natura sensibile, necessari per lo svolgimento delle mansioni lavorative, sono custoditi nell'archivio costituito dall'armadio, munito di serratura. Tali archivi potranno essere ad accesso controllato, per cui l'Incaricato può accedervi solo previa richiesta della chiave al Responsabile dei Trattamenti della propria Struttura di appartenenza, che durante l'orario lavorativo detiene la chiave stessa.

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

☐ richiedere la chiave per accedere all'archivio

Potrà essere istituito un "registro degli accessi all'archivio controllato", nel quale indicare la data e l'ora dell'accesso; descrivere sinteticamente le ragioni; apporre la propria firma in caratteri leggibili.

L'attribuzione di dispositivi e codici per accedere ai Personal Computer ed ai dati contenuti

Nello svolgimento dei suoi compiti, l'Incaricato potrà essere autorizzato ad accedere al Personal Computer a lui reso disponibile dall'Azienda, previa verifica della sua identità. A tale fine:

☐ all'Incaricato viene fornito, dall'Amministratore del sistema, un codice di identificazione (*username*), che dovrà provvedere a mantenere segreto. Qualora avesse il sospetto che terzi siano venuti a conoscenza dello stesso, dovrà informarne immediatamente il Responsabile dei Trattamenti della propria Struttura di appartenenza.

☐ gli viene fornita una parola chiave (*password*), composta di almeno otto caratteri alfanumerici, che dovrà provvedere a modificare in occasione del primo accesso al P.C., e successivamente almeno ogni sei mesi, nel caso in cui tratti solo dati di natura comune, o almeno ogni tre mesi, nel caso in cui tratti anche dati di natura sensibile o giudiziaria.

Si raccomanda di fare uso di caratteri sia alfabetici che numerici, che formino un codice non banale o facilmente individuabile.

La parola chiave deve essere:

a) mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia;

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

Supporti di tipo magnetico e/o ottico

La persona fisica designata e delegata al trattamento, ha l'obbligo di: 1) proteggere i dati personali archiviati su supporti di tipo magnetico e/o ottico con le stesse misure di sicurezza previste per i supporti cartacei; 2) verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro; 3) evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito; 4) assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione; 5) di rivolgersi tempestivamente, per difficoltà o questione inerente la sicurezza, al dirigente UOC.

Il reimpiego dei supporti di memorizzazione

Al termine dell'utilizzo dei dischetti, e degli altri supporti di memorizzazione contenenti datisensibili e/o di natura giudiziaria, questi dovranno essere consegnati al proprio diretto superiore gerarchico, che adotterà le procedure necessarie per cancellare ogni informazione contenuta in tali dischetti, prima di autorizzarne il reimpiego.

L'utilizzo dei software di protezione

Si raccomanda di utilizzare i software di protezione di cui dispone l'Azienda, le cui specifiche tecniche verranno fornite all'Incaricato, oltre che in questa sede, ogni volta che vi sono dei significativi aggiornamenti. Si sottolinea, in particolare, l'importanza di controllare metodicamente tutti i files (archivi elettronici) provenienti dall'esterno e di adottare diligentemente le opportune cautele, al momento della trasmissione all'esterno di files dell'Azienda.

L'utilizzo della posta elettronica

Per lo svolgimento delle mansioni lavorative, all'Incaricato potrà essere 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 dell'Incaricato.

La persona fisica designata e delegata al trattamento, al termine di ogni sessione di trattamento ha l'obbligo di uscire dall'applicazione utilizzata e di effettuare il logout.

L'utilizzo di Internet

Ad alcuni Incaricati, appositamente individuati dal diretto superiore gerarchico, verrà attribuito l'accesso ad Internet, del quale è consentito usufruire solo nei limiti strettamente necessari per lo svolgimento dell'attività lavorativa.

Si rammenta che è tassativamente vietato scaricare materiale e programmi in violazione della legislazione sui diritti di autore.

Prima di procedere allo scarico di qualsiasi file o programma, anche a titolo gratuito, dovrà inoltre chiedere l'autorizzazione al diretto superiore gerarchico.

Prescrizione residuale

Per dubbi ed incertezze, in merito a come debba avvenire il trattamento dei dati personali, l'Incaricato può rivolgersi al Responsabile dei Trattamenti della propria Struttura di appartenenza, per ricevere le dovute istruzioni.

Istruzioni ai sensi del GDPR e D.Lgs. n. 101/2018:

- in attuazione del principio di «liceità, correttezza e trasparenza», raccolta, registrazione, elaborazione di dati, agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati presenti nell'Ufficio di appartenenza, nell'osservanza delle tecniche e metodologie in atto;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui la persona fisica designata e delegata al trattamento è preposta;
- in attuazione del principio di «limitazione della finalità» trattamento conforme alle finalità istituzionali del titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, e obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione», obbligo di conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nell'Ufficio di competenza, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti

contenenti dati sensibili vengano conservati in contenitori/armadi muniti di serratura o in ambienti ad accesso selezionato e vigilato, fino alla restituzione;

- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente e integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- in attuazione del principio di «liceità, correttezza e trasparenza», autorizzazione a comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal titolare del trattamento.

DOCUMENTI	TEMPO DI CONSERVAZIONE
Accettazione donazioni	Illimitato
Ambulatori veterinari	Illimitato
Attestato di accettazione della pratica vaccinale	Illimitato
Atti di organi collegiali	Illimitato
Atti nomina e costituzione di Organi	Illimitato
Atti ricognitivi di Enti confluiti nell'Azienda U.S.L.	Illimitato
Bilanci	Illimitato
Carteggio vario sulle problematiche ambientali	Illimitato
Cartelle cliniche	Illimitato
Cartelle personali utenti servizi sociali	Illimitato
Certificazioni invalidi civili	Illimitato
Certificazioni medico legali (astensione anticipata dal lavoro per gravidanza, visite per idoneità al lavoro) e referti medici o risultati di accertamenti sanitari eseguiti su singoli lavoratori	Illimitato
Circolari in originale	Illimitato
Contabilità e corrispondenza relativa posizioni previdenziali e assistenziali	Illimitato
Contenzioso (documenti concernenti ricorsi giurisdizionali e amministrativi	Illimitato
Contratti e polizze	Illimitato
Contratti vari (manutenzione)	Illimitato
Corrispondenza con ISPESL (autorizzazioni)	Illimitato
Corrispondenza con vigili del fuoco (licenze, autorizzazioni e certificati)	Illimitato
Corrispondenza con il catasto (denunce)	Illimitato
Corrispondenza con Prefettura, Comuni, Regione, Stato (certificazioni autorizzazioni)	Illimitato
Corrispondenza con Organi di Stato (Uffici Giudiziari, Prefettura, Questura, Carabinieri, Organi di Polizia, Corte dei Conti, Ministeri e Uffici amministrativi dello Stato	Illimitato
Corsi di formazione del personale	Illimitato
Curriculum, azioni legali e ricorsi, documenti relativi all'inquadramento, visite medico collegiali, aspettativa senza assegni, infortuni sul lavoro, malattie professionali, certificati di servizio di altri Enti, docenze	Illimitato
Deliberazioni	Illimitato
Denuncia Ente (modello 770)	Illimitato
Documentazione relativa a segnalazioni dell'Autorità Giudiziaria	Illimitato
Documentazione relativa allo stato giuridico delle farmacie pubbliche e private, documentazione relativa alla sostituzione del titolare della farmacia, comunicazione di assunzione e cessazione degli addetti al servizio farmaceutico: albo nazionale dei titolari di farmacia e di archivio dei dati, erogazione indennità e contributi alle farmacie rurali ed ai dispensari farmaceutici, istruttorie amministrative espletate per provvedimenti di competenza del Sindaco	Illimitato
Documentazione concernente collaudi: regolare esecuzione e dichiarazione di conformità	Illimitato

Documentazione concernente gli accordi di lavoro: circolari applicative nazionali e regionali	Illimitato
Domande di riconoscimento della invalidità e relativi fascicoli	Illimitato
Donazioni	Illimitato
Esposti lamentele utenti	Illimitato
Fascicoli aziende	Illimitato
Fascicoli borsisti	Illimitato
Fascicoli contenenti gare d'appalto di opere pubbliche, edilizia sanitaria (dalla fase di avviamento a quella di aggiudicazione)	Illimitato
Fascicoli dei detentori di apparecchi radiologici	Illimitato
Fascicoli e verbali relativi a procedure concorsuali, di mobilità, di avvisi pubblici per incarichi, borse di studio, procedure afferenti attività di aggiornamento, etc……	Illimitato
Fascicoli personale dipendente e cessato	Illimitato
Fascicoli posizioni personali: medici di base, specialisti pediatri, medici servizio guardia medica, specialisti convenzionati esterni, specialisti e presidi convenzionati	Illimitato
Fatture emesse a vario titolo	Illimitato
Fuori uso e alienazione di beni mobili	Illimitato
Graduatorie e conferimenti (zone carenti medici di base e pediatri, incarichi vacanti di guardia medica, incarichi indeterminati e specialistici	Illimitato
Inchieste per infortuni sul lavoro	Illimitato
Inchieste per malattie professionali	Illimitato
Inventario beni	Illimitato
Istanze lavoratori CEE e non	Illimitato
Liquidazioni effettuate a vario titolo	Illimitato
Mangimifici	Illimitato
Manutenzioni straordinarie: aggiudicazione dei lavori e contabilità	Illimitato
Movimento demografico dati vaccinali	Illimitato
Notizie di reato e sanzioni amministrative	Illimitato
Offerte, domande di partecipazione e documentazione allegata alle ditte che vogliono partecipare a gare di appalto, licitazioni e trattative private	Illimitato
Ordinanze del Sindaco	Illimitato
Originali atti deliberativi	Illimitato
Pareri diversi espressi a richiesta del Sindaco a fini autorizzativi	Illimitato
Pareri espressi sui progetti edilizi	Illimitato
Pareri igienico sanitari	Illimitato
Posizione clinica pazienti ambulatoriali	Illimitato
Pratiche manuali di inventario relative ad ogni bene	Illimitato
Pratiche prelievi e trapianti organi	Illimitato
Pratiche relative a tirocinanti volontari	Illimitato
Procedimenti disciplinari	Illimitato
Progetti stalle	Illimitato
Referti analitici di laboratorio	Illimitato
Registri chiamate Guardia Medica	Illimitato

DOCUMENTI	TEMPO DI CONSERVAZIONE
Registri corsi infermieri psichiatrici	Illimitato
Registri tumori	Illimitato
Registri delle consegne nei reparti	Illimitato
Registri di protocollo ed eventuali rubriche di protocollo	Illimitato
Registro movimento pazienti e foglio movimento giornaliero	Illimitato
Registri o giornali di casa libro mastro	Illimitato
Registri operatori	Illimitato
Registri ricoverati/tabulati DRG	Illimitato
Regolamenti interni	Illimitato
Regolamento e disciplina ferie farmacie	Illimitato
Relazione annuale del servizio	Illimitato
Richieste cartelle cliniche	Illimitato
Ricorsi e contenzioso in genere	Illimitato
Ruoli contributi	Illimitato
Ruoli stipendiali annuali	Illimitato
Stalle di sosta	Illimitato
Statistiche	Illimitato
Stato servizi medici	Illimitato
Verbali di gara	Illimitato
Verbali organi collegiali e commissioni	Illimitato
Tossicodipendenza	Illimitato
Cartelle sanitarie lavoratori dipendenti	30 anni
Schede personali dosimetriche	30 anni dall'ultima registrazione
Autorizzazioni libero professionali	20 anni
Cartelle libretti sanitari compresi i referti analitici di laboratorio dalla consegna all'interessato	20 anni
Contabilizzazione ECU	20 anni
Denunce igiene pubblica (malattie infettive morsicature ecc...)	20 anni
Documenti polizia mortuaria	20 anni
Indennità di abbattimento	20 anni
Mandati di pagamento e reversali d'incasso	20 anni
Manutenzioni ordinarie: aggiudicazione dei lavori e contabilità	20 anni
Piani di profilassi di Stato	20 anni
Referti pronto soccorso	20 anni
Richiesta e referti di visita medico legale e fiscale	20 anni
Visite ambulatoriali esterne	20 anni
Autorizzazioni in deroga a norme di legge	10 anni
Bollettari di cassa per quietanze manuali emesse fino al 1989 per riscossione di introiti vari (ticket, servizi resi, prestazioni a pagamento, copie cartelle, donazioni, rette, etc....)	10 anni
Bollettari raccomandate	10 anni
Bollettari tesoreria	10 anni
Buoni d'ordine (acquisti)	10 anni
Carteggio altri servizi	10 anni

DOCUMENTI	TEMPO DI CONSERVAZIONE
Carteggio servizio telefonia	10 anni
Cartelle ambulatoriali	10 anni
Cartellini marcatempo specialisti convenzionati interni	10 anni
Cedolini paga	10 anni
Certificati di sana e robusta costituzione	10 anni
Contratti di manutenzione	10 anni
Contravvenzioni	10 anni
Copia modelli E 111 e similari – fascicoli attivati per assistenza e addebiti	10 anni
Copia distinte liquidazione contenenti: bolle in originale, copie fatture, ordini, ordinativi di pagamento economati, ordinanze di liquidazione, copie deliberazioni di liquidazione	10 anni
Copie autorizzazioni ricovero presso case di cura accreditate	10 anni
Denunce semestrali ai sensi dell'art. 22 della legge 482/68	10 anni
Dichiarazione dei redditi (modello 740)	10 anni
Distinte contabili delle farmacie e relativi controlli	10 anni
Distinte e impegnative delle prestazioni effettuate da convenzionati esterni	10 anni
Documentazione corsi aggiornamento medici	10 anni
Documentazione e pratiche per esenzione ticket rilasciate a qualsiasi titolo	10 anni
Documenti per attività di consulenza	10 anni dalla cessazione
Documenti relativi all'IVA e all'IRPEF	10 anni
Documentazioni relative a verifiche, controlli, raccolta dati su prescrizioni farmaceutiche	10 anni
Esposti	10 anni
Estratti conto tesoreria	10 anni
Farmaco vigilanza	10 anni
Fascicoli relativi a gare d'acquisto: materiali di consumo e attrezzature (comprendenti tutta la documentazione dalle richieste dei singoli servizi, all'espletamento della gara e all'avvio dell'ordine)	10 anni
Fascicoli delle deliberazioni (comprendenti tutto l'iter dell'atto deliberativo, dalla fase della proposta sino alla sua esecutività ed adempimenti connessi)	10 anni
Fascicoli relativi a morsi di animale	10 anni
Fascicoli pratiche macellazioni d'urgenza	10 anni
Fascicoli schede di stalle chiuse	10 anni
Fatturazione	10 anni
Fatturazione all'INAIL del compenso spettante all'A.U.S.L. relativamente alle certificazioni degli infortuni sul lavoro	10 anni
Frontespizi ricettari consegnati	10 anni
Gestione denaro pazienti	10 anni
Giornali di cassa, giornali corredati dalla data di versamento in originale e del riepilogo giornaliero IVA	10 anni

DOCUMENTI	TEMPO DI CONSERVAZIONE
Ispezioni: 1. accertamenti tecnico sanitari rilasciati in funzione di pareri previsti dalla legge; 2. accertamenti tecnico sanitari rilasciati a domanda per interessi di privati; 3. accertamenti tecnico sanitari rilasciati in funzione di attività obbligatoria di controllo;	10 anni
Lastre endorali per RX effettuate dall'odontoiatria	10 anni
Lastre radiografiche	10 anni
Matrici e buoni benzina per prelevamento carburanti	10 anni
Missioni	10 anni
Movimento giornaliero dei malati	10 anni
Offerte di ditte partecipanti a gare e non risultate aggiudicatarie di appalti	10 anni
Ordini di servizio	10 anni
Patenti di guida speciali	10 anni
Posizione personale libero professionale	10 anni
Pratiche amministrative per ricoveri con diritto a rimborso della retta (stranieri)	10 anni
Pratiche manutentive varie, con particolare riferimento agli interventi gratuiti ed in garanzia	10 anni
Progetti per nuovi insediamenti – pareri preventivi – pareri per agibilità e risposte alle notifiche	10 anni
Quietanze di cassa informatizzate o manuali per riscossioni varie comprese le operazioni commerciali (IVA)	10 anni
Quote aggiunta di famiglia e assegno nucleo familiare	10 anni
Refertari – copia del referto rilasciato dallo specialista all'utente dopo l'effettuazione delle prestazioni	10 anni
Referti ambulatoriali	10 anni
Referti analitici richiesti per il rilascio di certificazioni di sana e robusta costituzione	10 anni
Referti diagnostici EEG – ECG	10 anni
Registri ambulatoriali	10 anni
Registri consegne infermieristiche	10 anni
Registri decessi (comunicazioni autorità giudiziaria)	10 anni
Registri di carico e addebito documenti stupefacenti	10 anni
Registri e documenti alcolici ed idrocarburi	10 anni
Registri esami laboratorio e radiologia	10 anni
Registri rubricati con nominativo paziente trattato	10 anni
Registro corrispettivo per incassi riguardanti IVA	10 anni
Registro del volontariato e dei soggetti privati	10 anni
Registro macellazione animali	10 anni
Registro donatori	10 anni
Rendiconto obiettori	10 anni
Richiesta di accertamento di alloggio inidoneo e relativo referto	10 anni
Sequestri	10 anni
Tabulati stipendi specialisti ambulatoriali interni	10 anni
Tariffario	10 anni

DOCUMENTI	TEMPO DI CONSERVAZIONE
Trasfusioni	10 anni
Vaccinazioni	10 anni
Verbali: 1. sanzioni amministrative; 2. denunce autorità giudiziaria; 3. di sequestri: amministrativi, sanitari e penali.	10 anni
Verbali di ispezione	10 anni
Verbali ispezioni e controlli armadi farmaceutici	10 anni
Domande e documentazioni prodotte unitamente alla domanda di partecipazione a concorsi (prove e corrispondenza relativa, etc...) previa restituzione ai partecipanti, dei titoli presentati dall'approvazione della graduatoria	6 anni Dall'approvazione della graduatoria ad esclusione delle procedure con ricorsi pendenti
Atti necroscopici	5 anni
Acquisizione beni in conto visione	5 anni dalla restituzione
Albo dei fornitori con relativa documentazione e corrispondenza	5 anni
Avvisi interni e graduatorie	5 anni
Bolle di accompagnamento ora documenti di trasporto originali	5 anni
Bollettari beni viaggianti	5 anni
Bollettari documenti di trasporto beni viaggianti	5 anni
Bollettari riscossione suini macellati a domicilio	5 anni
Bollettari in genere	5 anni
Bollette per prestazioni specialistiche effettuate nell'ambito dei sevizi ed ambulatori dell'Azienda U.S.L. con allegata prescrizione proposta dal medico richiedente	5 anni
Buoni acquisto stupefacenti	5 anni
Certificati rilascio patenti	5 anni
Certificati porto d'armi	5 anni
Certificati trasporto animali e certificati sanitari carni	5 anni
Certificati di comodato gratuito per uso apparecchiature	5 anni dalla restituzione
Copia mandati di pagamento trasmessi al Servizio Gestione Economico Finanziaria	5 anni
Copie di referto di pronto soccorso ai fini del quantificato delle prestazioni con l'identificazione del pagamento del ticket per le prestazioni non urgenti erogate in detta sede	5 anni
Copie delle certificazioni medico legali rilasciate dal pronto soccorso ad infortunati sul lavoro assicurati INAIL	5 anni
Copie fatture emesse	5 anni
Corrispondenza attinente agli organi collegiali (convocazioni, commissioni medico legali, collegio dei Sindaci Revisori, etc...)	5 anni
Distinte e spese liquidate con ordinanza	5 anni
Distinte prestazioni extra	5 anni dal pagamento
Documentazione contabile relativa a comandi, trasferimenti, mobilità, missioni	5 anni
Documentazione sui turni vacanti specialisti convenzionati interni	5 anni
Documentazione concernente la fase preliminare delle procedure di gara per l'aggiudicazione dei prodotti farmaceutici	5 anni

Documentazione per ripartizione fondi, contributi ed altre entrate	5 anni
Documenti di scelta e revoca del medico	5 anni dalla cessazione
Domande utenti iscrizione al S.S.N.	5 anni
Donazione sangue	5 anni
Elementi accessori, lavoro straordinario, reperibilità, attività produttiva, proventi, indennità di rischio, missioni e trasferte, documentazione contabile	5 anni
Elenchi mensili dei pagamenti stipendi per la banca tesoriere	5 anni
Esiti per campione di sangue, compravendita e risanamento	5 anni
Estratti conti bancari e matrici blocchetti assegni (cassa economale)	5 anni
Fascicoli assistenza protesica ad invalidi	5 anni dal decesso dell'invalido
Graduatoria locale di A.U.S.L. guardia medica	5 anni
Listini per contratto fatture fornitori	5 anni
Matrici bollettari ricette farmaceutiche	5 anni
Moduli prescrizioni visite e analisi del medico di base o dei medici dell'A.U.S.L.	5 anni
Piani di lavoro per attività libero professionale svolta dai sanitari, corredata dalle bollette di prenotazione firmata dai medici a conferma dell'avvenuta prestazione	5 anni
Piani di profilassi malattie infettive	5 anni
Pratiche per degenti votanti nei presidi ospedalieri	5 anni
Pratiche inerenti l'erogazione di sussidi economici	5 anni
Pratiche per ricoveri a carico del S.S.N.	5 anni
Registri turni personale	5 anni
Registro di carico e scarico (bollettari, bolle di accompagnamento buoni mensa e relativi buoni di consumazione pasti)	5 anni
Registro cassa economale	5 anni
Registro carico e scarico rifiuti speciali	5 anni
Rendicondazione contabile mensile e fatturazione trimestrali degli accertamenti periodici eseguiti per conto delle strutture convenzionate	5 anni
Ricette fustellate	5 anni dal pagamento
Ricevute per pagamento ticket	5 anni
Ricevute vaccinazioni suini, bovini – copie profilassi risanamento	5 anni
Richieste di copie di deliberazioni e di motivazioni delle scelte fatte	5 anni
Richieste ferie, permessi, congedi straordinari, certificati di malattia, visite fiscali, permessi di studio e permessi sindacali	5 anni
Tabulati regionali mensili, attività di base e pediatrica con relativa documentazione di scelta e revoca	5 anni
Turni del personale	5 anni
Verbali di consegna dei bollettari di cassa	5 anni
Certificati movimento importazione ed esportazione animali	3 anni
Distinte notifiche di ricovero all'INPS – INAIL.	3 anni
Matrici ricettari riconsegnate dai medici prescriventi	3 anni

DOCUMENTI	TEMPO DI CONSERVAZIONE
Osservatorio prezzi, documentazione costituita da dischetti e tabulati	3 anni
Registro anticipi erogati a personale avente diritto per missioni e relative copie del foglio di missione	3 anni
Ricette veterinari, libero professionisti, farmaci veterinari per detenzione scorte etc....	3 anni
Richiesta copie cartelle cliniche	3 anni
Risultati dei controlli di qualità esterni	3 anni
Tabulati di verifica andamento dei consumi	3 anni
Tabulati per mandati di pagamento, distinte etc....	3 anni
Congedi ordinari, ore straordinario, turni predisposti dalla direzione sanitaria per reperibilità personale medico e non medico guardia medica, giustificazioni per assenze inferiori alla durata di una giornata lavorativa e che comunque comportino la presenza in servizio nel giorno stesso, stampe CED, riepilogo assenze personale	2 anni
Copie referti, visite specialistiche ed esami diagnostici	2 anni
Documenti riguardanti prenotazioni per visite ed esami	2 anni
Matrici buoni benzina e blocchetti di prelievo carburanti presso fornitori	2 anni
Richieste dei servizi al magazzino centrale e relativi tabulati dei consumi per centro di costo	2 anni
Risultati di esami di laboratorio di utenti	2 anni
Schede per assistenza integrativa	2 anni
Stampa mensile delle presenze	2 anni
Tabulati di inventario dei beni mobili per centro di costo e tabulato generale	2 anni dall'ammissione

Azienda Sanitaria Provinciale di Enna
Viale Diaz n.7/9 94100 Enna
COD. FISC. E P.IVA: 01151150867

ATTO DI NOMINA A RESPONSABILE ESTERNO PER IL TRATTAMENTO DEI DATI PERSONALI

nell'ambito delle misure finalizzate a dare attuazione alle disposizioni del Regolamento (UE) n. 679/2016 (GDPR) e del D.Lgs n. 101/2018

Il/La sottoscritto/a _____ (Nome Cognome), in qualità di responsabile del trattamento dei dati ai sensi del GDPR 2016/679, in forza del contratto avente ad oggetto _____ stipulato in data _____ , si avvale del supporto di _____,
con sede legale in_____,
Codice Fiscale n. _____ e Partita IVA n. _____ (di seguito denominato "Responsabile esterno"), per la fornitura di _____ ;

NOMINA

il Sig./Sig.ra _____
(Nome Cognome) Responsabile esterno del trattamento dei dati, effettuato dalla Ditta _____presso la sede di _____
Via_____,
con strumenti elettronici, automatizzati o cartacei, nell'ambito delle attribuzioni, competenze e funzioni assegnate.

In qualità di Responsabile esterno del trattamento dei dati, il/la sig.sig.ra_____ ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto previsto dal GDPR, nonchè le seguenti istruzioni impartite dal Titolare.

COMPITI ED ISTRUZIONI PER I RESPONSABILI ESTERNI DEL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'art. 28 del Regolamento UE 2016/679.

PRINCIPI GENERALI DA OSSERVARE
Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:
per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del

Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di correttezza, che deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi:il trattamento ed il fine della raccolta dei dati deve essere lecito;
  - compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e, comunque, in osservanza delle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

L'atto propedeutico al trattamento è la sottoscrizione, da parte dell'interessato, dell'**informativa** (redatta ai sensi del GDPR) e del **consenso al trattamento**.
In particolare, i dati classificati come "SENSIBILI" (a mero titolo esemplificativo quelli idonei a rivelare lo stato di salute o la vita sessuale ed i dati giudiziari) sono conservati separatamente da altri dati personali.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.
Ciascun Responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste sanzioni penali.
In ogni caso, la responsabilità penale per un eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia

imputabile e, per l'effetto, l'A.S.P. di Enna ne risulta indenne.
In merito alla responsabilità civile, si fa rinvio all'art. 2043 e ss. del Codice Civile

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

a) acquisire il consenso informato e la sottoscrizione del modulo "Informativa al trattamento dei dati personali" ;
b) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;

c) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;

d) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

e) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa (completa di tutte le informazioni prescritte dal GDPR) ai soggetti interessati. A cura dei Responsabili dovranno inoltre essere affissi i cartelli contenenti l'informativa, in tutti i luoghi ad accesso pubblico, con la precisazione che l'informazione resa attraverso la cartellonistica integra ma non sostituisce l'obbligo di informativa in forma orale o scritta;

f) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;

g) adempiere agli obblighi di sicurezza, quali:

- adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee 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 della raccolta;
- definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati

in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

h) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;

i) collaborare con il Responsabile per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;

j) comunicare tempestivamente al Responsabile ogni notizia rilevante ai fini della tutela della riservatezza ed i casi di violazione della privacy;

Il Responsabile esterno del trattamento risponde all'ASPper ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è ad esclusivo carico della singola persona cui l'uso illegittimo sia imputabile.

L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali ed alle raccomandazioni del Garante privacy, che qui si richiamano integralmente.

Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico Il Responsabile esterno del trattamento (NOME COGNOME)	Il Responsabile designato dal titolare del trattamento (NOME COGNOME)
_____ (firma)	_____ (firma)