Stemma dell'Ospedale di S. Maria della Misericordia di Perugia

Azienda Ospedaliera di Perugia

Direzione Generale e Sede Ammin.va: Piazzale Menghini, 8/9 – 06129 PERUGIA
Sede Legale: Ospedale S. Maria della Misericordia – S. Andrea delle Fratte – 06156 PERUGIA
Part. IVA 02101050546 – tel.: 075/5781 – Sito Internet: www.ospedale.perugia.it
PEC: aosp.perugia@postacert.umbria.it

DELIBERAZIONE DEL DIRETTORE GENERALE
n. 0000076 del 27/01/2025
adottata in Perugia

OGGETTO:
AGGIORNAMENTO DEL "REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"

Ufficio Proponente: AFFARI GENERALI
Istruttore della pratica: ELEONORA MARIANI
Responsabile del procedimento: GLAUCO ROSSI
Dirigente dell'Ufficio Proponente: GLAUCO ROSSI
La Delibera comporta costi: No
Modalita' di Pubblicazione: Integrale

VISTA la proposta n. 0001594 del 30/12/2024 a cura di AFFARI GENERALI
hash.pdf (SHA256): e20671144a081ad181d530845973f20b201d90c92fe88daaf3067563e99b8e8d
firmata digitalmente da: GLAUCO ROSSI
che ne attesta la regolarita' dell'iter istruttorio

IL DIRETTORE SANITARIO: ARTURO PASQUALUCCI
Parere: FAVOREVOLE

IL DIRETTORE AMMINISTRATIVO: ROSA MAGNONI
Parere: FAVOREVOLE

DELIBERA

Di fare integralmente propria la menzionata proposta che allegata al presente atto ne costituisce parte integrante e di disporre così come in essa indicato, avendone acquisito i pareri

IL DIRETTORE GENERALE
GIUSEPPE DE FILIPPIS*

** Documento sottoscritto con firma digitale*

Stemma dell'Ospedale di S. Maria della Misericordia di Perugia

Azienda Ospedaliera di Perugia

Direzione Generale e Sede Ammin.va: Piazzale Menghini, 8/9 – 06129 PERUGIA
Sede Legale: Ospedale S. Maria della Misericordia – S.Andrea delle Fratte – 06129 PERUGIA
Part.IVA 02101050546 – tel.: 075/5781 fax: 075/5783531 PEC: aosp.perugia@postacert.umbria.it

S.C. AFFARI GENERALI

OGGETTO: Aggiornamento del "Regolamento in materia di protezione dei dati personali".

Visti:

il Decreto Legislativo n. 196 del 30.06.2003, "Codice in materia di protezione dei dati personali*"* e s.m.i.;

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 (regolamento generale sulla protezione dei dati*" (General Data Protection Regulation - GDPR), e* s.m.i.;

il Decreto Legislativo n. 101 del 10.08.2018, *"*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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" e s.m.i.;

la Deliberazione della Giunta regionale n. 1185 del 09 gennaio 2020 avente ad oggetto "Direttive in materia di trattamento dei dati personali – approvazione disciplinare privacy e linee guida ai sensi del Reg. UE n. 679/2016 e del d.lgs. 196/2003";

Premesso che l'Azienda Ospedaliera di Perugia, in quanto Titolare del Trattamento dei dati personali, agisce attraverso il Direttore Generale, suo rappresentate legale, per mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali sia effettuato conformemente al GDPR, così come stabilito dagli articoli 5, paragrafo 2 e 24, paragrafo 1, del Regolamento (UE) 2016/679;

Dato atto che la Direzione Aziendale ha dato mandato alla S.C. Affari Generali di procedere alla stesura e formalizzazione del *Regolamento in materia di protezione dei dati personali,* per dare attuazione agli obblighi ed adempimenti previsti dal GDPR;

Rilevato che il succitato Regolamento mira ad introdurre direttive applicative delle normative vigenti in materia di trattamento dei dati personali definendo il complessivo ambito delle responsabilità, dei ruoli e delle funzioni all'interno dell'Azienda, nonché gli indirizzi organizzativi e procedurali per l'attuazione dei trattamenti di dati personali, tenuto conto anche del modello organizzativo dell'Azienda, come rinnovato dalla Delibera del Direttore generale n. 288 del 07.03.2024;

Attestata la regolarità amministrativa del presente provvedimento ai sensi del D. Lgs n. 123/2011;

Direzione Generale e Sede Ammin.va: Piazzale Menghini, 8/9 – 06129 PERUGIA
Sede Legale: Ospedale S. Maria della Misericordia – S.Andrea delle Fratte – 06129 PERUGIA
Part.IVA 02101050546 – tel.: 075/5781 fax: 075/5783531 PEC: aosp.perugia@postacert.umbria.it

Attestato altresì che, a seguito dell'istruttoria effettuata, nella forma e nella sostanza la proposta è legittima ed utile per il sevizio pubblico;

Tutto ciò premesso e considerato,

SI PROPONE DI:

1) **Approvare**, per le motivazioni espresse in premessa che qui si intendono richiamate, il "Regolamento in materia di protezione dei dati personali", riportato in Allegato 1 come parte integrante del presente provvedimento.
2) **Trasmettere** il presente provvedimento a tutte le Strutture Complesse/Semplici Aziendali.
3) **Pubblicare,** a cura della Direzione Affari Generali, il presente Regolamento sul sito aziendale "Amministrazione Trasparente", sezione "Disposizioni Generali".

Il Funzionario Istruttore
Dott.ssa Eleonora Mariani

S.C. Affari Generali
Il Direttore f.f.
Dott.re Glauco Rossi

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Redatto da	Ufficio prevenzione della corruzione, trasparenza e trattamento dei dati personali	**Revisione n.:**	01
Verificato da	S.C. Affari Generali	**Data:**	19.12.2024
Pubblicazione	Amministrazione Trasparente – Disposizioni Generali – Atti Generali – Regolamenti Aziendali	**Data:**	30.01.2025

STORIA DELLE MODIFICHE APPORTATE

Data	Rev.	Motivo del cambiamento
29.12.2006	00	Prima emissione
	01	Aggiornamento normativo

INDICE

PREMESSA

Il presente Regolamento Aziendale in materia di protezione dei dati personali (da ora in poi, **Regolamento**) è stato predisposto per regolare, attraverso una serie di misure che compongono un vero e proprio "sistema gestionale privacy", i compiti e le responsabilità di tutti coloro che nell'Azienda Ospedaliera di Perugia (da ora in poi, **A.O.Pg**) trattano dati personali.

Il documento, che è stato elaborato tenendo conto dell'attuale quadro normativo, composto sia dal Regolamento UE 2016/679 sulla Protezione dei Dati Personali (da ora in poi, **GDPR** – GENERAL DATA PROTECTION REGULATION), sia dalle indicazioni del decreto legislativo n. 196/2003 così come adeguato dal decreto legislativo n. 101/2018 e s.m.i., costituisce la base del sistema di accountability, adottato dall'A.O.Pg nella sua veste di Titolare del trattamento, che sarà opportunamente implementato con tutte le misure derivanti da questo regolamento organizzativo.

DISPOSIZIONI DI RIFERIMENTO

- legge n. 241 del 07.08.1990, *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*, e s.m.i.;
- decreto legislativo n. 196 del 30.06.2003, *Codice in materia di protezione dei dati personali*, e s.m.i.;
- decreto legislativo n. 82 del 07.03.2005, *Codice dell'Amministrazione Digitale* e s.m.i.;
- deliberazione n. 88 del 02.03.2011 del Garante per la Protezione dei Dati Personali ad oggetto *"Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web"*;
- deliberazione n. 31 del 25.01.2012 del Garante per la Protezione dei Dati Personali ad oggetto *"Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute"*;
- decreto legislativo n. 33 del 14.03.2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*, e s.m.i;
- regolamento Regione Umbria n. 7 del 30.12.2013, *Trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, degli enti e delle agenzie regionali, delle aziende unità sanitarie locali, delle aziende ospedaliere, delle aziende ospedaliero-universitarie e degli altri soggetti pubblici per i quali la Regione esercita poteri di indirizzo e controllo.*

- *linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri Enti obbligati*, provvedimento n. 243 del 15 maggio 2014 del Garante per la Protezione dei Dati Personali;
- 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 (regolamento generale sulla protezione dei dati)*, e s.m.i.
- *linee guida sui responsabili della protezione dati (RPD)*, del Gruppo di Lavoro Articolo 29 in materia di protezione dei dati personali, versione emendata ed adottata il data 05.04.2017 (WP 243 rev. 01).
- *linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, del Gruppo di Lavoro Articolo 29 per la protezione dei dati, versione modificata ed adottata da ultimo il 04.10.2017 (WP 248 rev. 01).
- *linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, del Gruppo di Lavoro Articolo 29 per la protezione dei dati, versione emendata ed adottata in data 06.02.2018 (WP 250 rev. 01).
- *linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, del Gruppo di Lavoro Articolo 29 per la protezione dei dati, versione modificata ed adottata da ultimo in data 10.04.2018 (WP 259 rev. 01).
- *linee guida sulla trasparenza ai sensi del regolamento (UE) 2016/679*, del Gruppo di Lavoro Articolo 29 per la protezione dei dati, versione emendata adottata in data 11.04.2018 (WP 260 rev. 01).
- decreto legislativo n. 101 del 10.08.2018, *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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, e s.m.i.;

ART. 1 – OGGETTO E AMBITO DI APPLICAZIONE

Il presente documento individua le politiche aziendali relative alla corretta gestione del trattamento dei dati personali, così come definiti dal "Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", dal Decreto Legislativo 196/2003 "Codice in materia di

protezione dei dati personali" così come modificato dal Decreto Legislativo 101/2018 e dai Provvedimenti del Garante per la Protezione dei Dati, attraverso l'individuazione di una serie di misure che compongono un vero e proprio "Sistema Gestionale Privacy – SGP", nonché di compiti e di responsabilità di tutti coloro che nell'Azienda trattano dati personali.

Il documento è stato elaborato tenendo conto dell'attuale quadro normativo e contribuisce al miglioramento del sistema di accountability adottato dall'A.O.Pg, nella sua veste di Titolare del trattamento.

L'A.O.Pg si impegna ad implementarlo con tutte le necessarie misure da questo derivanti.

ART. 2 - PRINCIPI

L'A.O.Pg, anche in considerazione dell'estrema delicatezza dei dati personali che correntemente tratta, della loro molteplicità e della numerosità dei soggetti che necessariamente devono trattarli, adotta misure capaci di assicurare e documentare che il trattamento dei dati personali viene effettuato con modalità tali da preservarne l'integrità e la confidenzialità, nel rispetto delle adeguate misure di sicurezza.

A riguardo, l'A.O.Pg attiva le necessarie risorse organizzative, tecnologiche e finanziarie affinché il trattamento dei dati personali sia conforme alle disposizioni in materia di protezione dei dati e di amministrazione digitale, nell'osservanza dei seguenti principi, come sanciti nell'art. 5 del GDPR:

- **liceità, correttezza e trasparenza**: i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- **limitazione della finalità**: i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- **minimizzazione dei dati**: i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **esattezza**: i dati devono essere esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- **limitazione alla conservazione**: i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati, salvo che vengano conservati per periodi più lunghi ai soli fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate che tutelino i diritti e le libertà dell'interessato;

- **integrità e riservatezza**: i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- **responsabilizzazione**: il trattamento è effettuato in maniera conforme alla normativa così da non determinare rischi e, quindi, gravare sui diritti e le libertà degli Interessati.

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Inoltre i dati sono trattati in modo lecito se il trattamento rispetta:

- i presupposti e limiti stabiliti dalla normativa vigente e dalle disposizioni del Garante;
- le eventuali disposizioni contenute nei codici di deontologia e di buona condotta;
- adeguate misure di sicurezza;
- le normative di settore (a titolo esemplificativo: osservanza del segreto professionale, rispetto della riservatezza in materia di interruzione della gravidanza o di tossicodipendenza o di soggetti HIV).

ART. 3 – RISPETTO DEI CODICI DEONTOLOGICI

L'Azienda promuove il rispetto, da parte dei propri professionisti iscritti in albi professionali, delle disposizioni contenute nei rispettivi codici deontologici. Qualunque trattamento di dati

personali deve essere effettuato in ottemperanza a quanto in essi stabilito, pena la non liceità del trattamento stesso.

ART. 4 – ACCOUNTABILITY E SISTEMA GESTIONALE DELL'A.O. PG.

L'A.O. Pg mette in atto tutte le misure tecniche ed organizzative adeguate per garantire e dimostrare come il trattamento dei dati personali sia stato effettuato conformemente alla normativa vigente, in considerazione del possibile rischio di lesione dei diritti e delle libertà degli Interessati, tenuto conto della natura, nonché dell'ambito di applicazione, del contesto e delle finalità del trattamento stesso.

Tali misure sono riesaminate e aggiornate periodicamente e, se proporzionata rispetto all'attività di trattamento, tra di esse rientra l'adozione di politiche adeguate in materia di protezione dei dati.

Il Sistema di Gestione Privacy (SGP) aziendale, quindi il complesso di documenti, regole, formazione e procedure di controllo omogeneo ed integrato, di cui l'A.O.Pg si è dotata, include:

- il Gruppo di Coordinamento per la Protezione dei Dati (GCPD) (vd. infra art. 24);
- il Registro delle attività di trattamento dei dati (vd. infra art. 16);
- il sistema di attribuzione delle responsabilità del trattamento dei dati personali (vd. infra artt. 17-24),
- la documentazione relativa alle informative ed al rilascio delle autorizzazioni al trattamento dei dati (vd. infra artt. 25-27);
- la documentazione relativa alle valutazioni di impatto (vd. infra art. 30);
- le regolamentazioni, le policy, le procedure e le disposizioni operative adottate;
- il sistema di audit e verifica periodica del corretto trattamento dei dati personali;
- il sistema di gestione delle violazioni dei dati personali (vd. infra art. 38);
- il sistema di formazione continua dei Responsabili designati al trattamento, Autorizzati al trattamento ed Amministratori di sistema (vd. infra art. 37);

L'A.O.Pg perfeziona, in un'ottica proattiva e di rispetto dei bisogni e dei diritti, il SGP al fine di realizzare un sistema integrato in evoluzione continua con l'obiettivo di rendere l'innovazione e la revisione organizzativa dei processi sanitari un investimento fondamentale per migliorare il rapporto costo-qualità dei servizi sanitari e la qualità percepita dal cittadino che ne usufruisce.

ART. 5 – CATEGORIE DI INTERESSATI E DI DATI PERSONALI TRATTATI

L'A.O.Pg tratta i dati personali relativi a:

- cittadini utenti, assistiti e loro familiari e/o accompagnatori;
- personale in rapporto di dipendenza, convenzione o collaborazione;
- soggetti che per motivi di studio o volontariato frequentano le strutture dell'A.O.Pg;
- clienti e fornitori.

I dati personali trattati comprendono anche le categorie di dati particolari (sensibili), con particolare riferimento a:

- dati idonei a rivelare lo stato di salute e la vita sessuale;
- dati genetici;
- dati biometrici.

Nei casi e con i limiti previsti dalle normative di settore vigenti, l'A.O.Pg, altresì, tratta dati personali e particolari, come la rilevazione delle malattie mentali, infettive e diffusive e della sieropositività, a fini di indagini epidemiologiche, di trapianto di organi e tessuti e/odi monitoraggio della spesa sanitaria; questi sono trattati qualora siano essenziali e necessari allo svolgimento delle attività istituzionali e nel caso in cui tali attività non possano essere adempiute mediante il trattamento di dati pseudonimizzati o di dati personali di natura diversa.

I dati personali trattati dall'A.O.Pg, nelle forme e nei limiti di quanto previsto dalla normativa vigente, sono raccolti:

- direttamente presso l'interessato, o anche presso persone diverse, nei casi in cui questi sia minorenne o incapace o non sia in grado di fornirli;
- anche presso enti del SSN, altri enti e amministrazioni pubbliche o terzi, pubblici registri, o presso altri esercenti professioni sanitarie.

Per effettuare il trattamento dei dati personali, l'A.O.Pg utilizza sistemi manuali e automatizzati.

Il trattamento dei dati personali per fini di ricerca scientifica o statistica viene effettuato con il consenso dell'interessato o, negli altri casi previsti dalla normativa vigente, soltanto previa erogazione di apposita informativa ed adozione di apposite ed adeguate misure di sicurezza.

I risultati della ricerca pubblicati o comunque resi noti non possono in alcun caso contenere dati personali che rendano identificabili i soggetti ai quali si riferiscono.

ART. 6 – FINALITÀ E MODALITÀ DEL TRATTAMENTO DEI DATI PERSONALI

I trattamenti di dati personali effettuati dall'A.O.Pg sono finalizzati:

- allo svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico e all'espletamento delle funzioni istituzionali previste dalle normative vigenti;
- all'erogazione di prestazioni sanitarie specialistiche, sia istituzionali che di libera professione intramuraria (comprensive di tutte le attività di supporto), volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;
- allo svolgimento di funzioni di assistenza sanitaria, didattica, formazione e ricerca scientifica, statistica ed epidemiologica, finalizzata alla tutela della salute;
- alla tutela della sicurezza e della salute dei lavoratori e sorveglianza igienico-sanitaria delle proprie strutture;
- alla gestione delle proprie risorse umane, tecnologiche, strumentali e patrimoniali in quanto soggetto aziendale;
- alla tutela del proprio patrimonio aziendale.

Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento dei dati, dei Responsabili (interni ed esterni) designati e degli eventuali sub-responsabili, degli Autorizzati e degli Amministratori di Sistema.

All'interno dell'A.O.Pg sono individuati i ruoli e i compiti dei soggetti autorizzati a trattare i dati di pertinenza del Titolare del trattamento dei dati personali ed è illecito il trattamento di dati personali da parte di soggetti che non siano stati a ciò preventivamente e formalmente autorizzati dall'A.O.Pg.

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'Interessato ed oggetto del trattamento possono essere i soli dati essenziali e necessari per svolgere le attività istituzionali.

I dati personali devono essere trattati dai Responsabili interni ed esterni designati, dagli Autorizzati e dagli Amministratori di Sistema in modo lecito, sono raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini non incompatibili con tali scopi.

I Responsabili designati al trattamento sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati personali, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa.

I Responsabili designati, gli Autorizzati e gli Amministratori di Sistema sono autorizzati all'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento dei dati personali è consentito.

I Responsabili designati sono tenuti a comunicare dati personali e/o particolari agli altri Responsabili designati al trattamento solo in caso di necessità, ovvero quando non sia possibile perseguire le stesse finalità con dati anonimi o aggregati.

I dati personali possono essere oggetto di conservazione sia analogica che digitale solo per il tempo previsto dalla normativa vigente e successivamente sottoposti a scarto d'archivio o distruzione.

In particolare, i Responsabili designati relativamente alla gestione, protezione e manutenzione dei sistemi informativi e dei programmi informatici dovranno assicurare al Titolare del trattamento che tali sistemi e programmi siano pre-configurati in ossequio al principio della *privacy by design* (privacy come criterio di progettazione di un trattamento) *and by default* (privacy per impostazione predefinita), quindi progettati per soddisfare le garanzie indispensabili di tutela dei diritti degli Interessati tenendo conto del contesto complessivo nel quale il trattamento viene svolto e dei rischi per i diritti e le libertà degli Interessati. L'applicazione di tale criterio assicura la riduzione al minimo dell'impiego di dati personali ed identificativi, così da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o procedure che permettano l'identificazione dell'interessato solo in caso di necessità.

I dati che, anche a seguito di verifica, risultino eccedenti o non pertinenti o non necessari non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.

I trattamenti di dati effettuati utilizzando le banche dati di più Titolari, sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge o previa specifica autorizzazione da parte dell'Autorità Garante.

ART. 7 – TRATTAMENTO DEI DATI PERSONALI

In base a quanto stabilito all'art. 6 del Regolamento UE 2016/679, l'A.O.Pg tratta i dati personali solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

La base su cui si fonda il trattamento dei dati di cui alle lettere c) ed e), deve essere stabilita dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui alla lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Laddove il trattamento, per una finalità diversa da quella per la quale i dati personali sono stati raccolti, non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione, o degli Stati membri, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 del Regolamento UE 2016/679, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 del Regolamento UE 2016/679;

d) delle possibili conseguenze, per gli interessati, dell'ulteriore trattamento previsto;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

ART. 8 – TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI NECESSARIO PER MOTIVI DI INTERESSE PUBBLICO RILEVANTE

I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento UE, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Ai sensi dell'art. 2-sexies del d.lgs. 196/2003 e s.m.i., si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nella materia di cui alla lettera u) del medesimo articolo: compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile salvaguardia della vita e incolumità fisica.

Con riferimento ai compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, il regolamento 30.12.2013 n. 7 della Regione Umbria (*Trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, degli enti e delle agenzie regionali, delle aziende unità sanitarie locali, delle aziende ospedaliere, delle aziende ospedaliero-universitarie e degli altri soggetti pubblici per i quali la Regione esercita poteri di indirizzo e controllo)*, nell'allegato B, identifica i tipi di dati e le operazioni eseguibili dalle aziende ospedaliere nello svolgimento delle loro funzioni istituzionali con riferimento ai trattamenti di dati "sensibili e giudiziari" effettuati per il perseguimento delle rilevanti finalità di interesse pubblico.

ART. 9 – TRATTAMENTO DEI DATI PARTICOLARI

L'A.O.Pg tratta dati personali che rivelano l'origine razziale o etnica, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita o all'orientamento sessuale della persona soltanto se:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
e) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita;
f) il trattamento è necessario per rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali o conformemente al contratto con un professionista della sanità;
h) il trattamento è necessario per motivi di interesse di ordine pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
i) il trattamento è necessario ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Qualora il trattamento sia basato sul consenso, è compito dell'A.O.Pg dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento e ciò non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

ART. 10 – TRATTAMENTO DEI DATI SOTTOPOSTI A MAGGIOR TUTELA

Il trattamento dei dati relativi alle seguenti informazioni è sottoposto ad un regime normativo di particolare tutela:

- sieropositività;
- interruzione volontaria di gravidanza;
- vittime di violenza sessuale o di pedofilia;
- uso di sostanze stupefacenti o psicotrope e di alcool;
- parto in anonimato.

L'A.O.Pg tratta tali tipologie di dati garantendo l'adempimento dell'obbligo di un trattamento dei dati non immediatamente identificativi della persona, che si realizza, di norma, attraverso l'utilizzo di codici alfanumerici, che comunque il Titolare, il Responsabile, ovvero gli autorizzati a ciò specificatamente autorizzati, hanno la possibilità di ricondurre ad un soggetto determinato.

L'A.O.Pg è impegnata a favorire fra gli operatori l'adozione di comportamenti corretti improntati alla massima attenzione e cautela nel trattamento di dette tipologie di dati.

ART. 11 – TRATTAMENTO DEI DATI GIUDIZIARI

Il trattamento di dati giudiziari è ammesso se indispensabile per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. Il trattamento dei dati giudiziari, compresa la loro comunicazione, è 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 rilevanti finalità di interesse pubblico perseguite.

ART. 12 – OBBLIGHI DI TRASPARENZA

L'Azienda assolve agli obblighi di legge in materia di trasparenza, quale livello essenziale delle prestazioni concernenti diritti civili e sociali ai sensi dell'art.117, lettera m) della Costituzione, con la pubblicazione sul proprio sito internet istituzionale dei dati di cui al D.Lgs. n. 33/2013, nel rispetto delle linee guida impartite dal Garante per la protezione dei dati personali.

ART. 13 – REDAZIONE DEGLI ATTI, PUBBLICITÀ' E TUTELA DELLA TRASPARENZA

I responsabili delle strutture organizzative che propongono una deliberazione o che adottano una determinazione dirigenziale con il supporto tecnico dei relativi responsabili del procedimento verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dalla

normativa, 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 particolari in sede di pubblicazione all'Albo on-line 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.

ART. 14 – POLITICHE DI ACCESSO AI DATA-BASE E PROFILI DI AUTORIZZAZIONE

Nel rispetto del principio di necessità e pertinenza del trattamento dei dati personali, i profili di accesso ai gestionali informatici aziendali sono configurati sulla base delle attività affidate a ciascun incaricato e nel rispetto degli ambiti di trattamento consentiti.

L'assegnazione dei predetti profili ai singoli operatori autorizzati del trattamento dei dati è effettuata a cura dei rispettivi Responsabili interni ed esterni designati al trattamento dei dati.

Per ciascuna banca dati (applicativo informatico) deve essere definito l'elenco dei profili di accesso e le loro specificità.

Le finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria (a titolo esemplificativo: prenotazione e pagamento di una prestazione) devono essere realizzate garantendo il principio della necessità del trattamento e quindi precludendo, per quanto possibile, l'accesso del personale amministrativo alle informazioni sanitarie, mediante la previsione di profili diversi di abilitazione in funzione della diversa tipologia di operazioni consentite.

In ogni caso gli accessi ai dati personali contenuti nei data base aziendali devono essere ridotti allo stretto necessario per consentire l'espletamento delle ordinarie attività lavorative.

Il trattamento dei dati deve, pertanto, essere evitato ogni volta in cui lo stesso non sia indispensabile per il perseguimento degli scopi prefissati.

Periodicamente i Responsabili designati al trattamento curano l'aggiornamento dei profili di autorizzazione del personale assegnato.

Al fine di garantire che il trattamento dei dati inerenti allo stato di salute degli interessati sia effettuato con un idoneo livello di sicurezza, gli accessi ai software clinici devono essere tracciati.

ART. 15 – STRUMENTI DI VIDEOSORVEGLIANZA E VIDEO-MONITORAGGIO

L'installazione di apparecchiature di videosorveglianza è autorizzata dal Titolare, previo accordo con le organizzazioni sindacali, solo quando ciò sia strettamente indispensabile per la sicurezza delle persone e delle attrezzature (controllo di corridoi, di sale di attesa, di spazi esterni, di porte di accesso agli edifici, altro) e non siano attuabili o sufficienti altre misure di sorveglianza.

Il trattamento dei dati personali con le apparecchiature di cui sopra è effettuato nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori e delle prescrizioni del Garante per la Protezione dei Dati Personali.

Per tutti i sistemi di controllo attivati dall'A.O.Pg, questa deve assicurare l'effettività delle misure di tutela degli interessati e dei lavoratori, in particolare per quanto riguarda l'erogazione di specifica informativa e la piena trasparenza delle caratteristiche, finalità e modalità del controllo operato.

Il Titolare fornisce al Responsabile del trattamento le istruzioni necessarie sulle modalità di trattamento dei dati raccolti con le apparecchiature di videosorveglianza, sulle misure di sicurezza da osservare, nonché sull'informativa da fornire agli utenti, agli operatori e alle altre persone che a qualsiasi titolo accedono agli spazi sorvegliati, in relazione alle finalità e alla tipologia del sistema di sorveglianza.

L'attività di video-monitoraggio, che si distingue rispetto alle attività di videosorveglianza propriamente dette, ha particolari finalità, come, a titolo esemplificativo, quella relativa alla sorveglianza remota di pazienti ricoverati, per esclusive finalità di cura e tutela della salute.

Tale attività non prevede ordinariamente la registrazione di immagini. Possono accedere alle immagini rilevate per le predette finalità solo i soggetti specificatamente autorizzati (personale medico e infermieristico, o altro).

Le immagini idonee a rilevare lo stato di salute non possono essere diffuse.

ART. 16 – REGISTRO DELLE ATTIVITÀ' DI TRATTAMENTO DEI DATI PERSONALI

Il Registro dei Trattamenti è l'atto fondamentale attraverso il quale vengono censiti i trattamenti di dati personali, al fine di analizzarne le caratteristiche, valutarne i rischi e programmare le misure di sicurezza.

L'A.O.Pg individua come elementi fondamentali delle politiche di protezione dei dati personali:

- l'analisi dei trattamenti di dati personali;

- la distribuzione dei compiti e delle responsabilità attribuite a coloro che trattano dati personali.

L'A.O.Pg provvede, inoltre, alla rilevazione dei trattamenti dei dati personali suddivisi per tipologia e per struttura organizzativa e ogni altro elemento necessario ad individuare le responsabilità relative al loro trattamento.

L'A.O.Pg tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato a cura del Titolare, tramite i Responsabili designati, che evidenzia i diversi livelli di responsabilità attribuiti in relazione al trattamento dei dati e contiene le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del Responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento UE, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Tale registro viene tenuto anche dai Responsabili esterni e Sub-responsabili esterni del trattamento.

Il registro è tenuto in forma scritta, anche in formato elettronico mediante apposita piattaforma gestionale e, su richiesta, viene messo a disposizione dell'Autorità Garante Privacy.

Il Titolare ed i Responsabili designati hanno le loro credenziali di accesso al Registro, con specifici poteri, al fine di tenere costantemente aggiornato il Registro e provvedere agli altri adempimenti connessi, quali ad esempio la nomina e relativa annotazione dei responsabili esterni e l'autorizzazione al personale incaricato del trattamento.

ART. 17 – TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

Il Titolare del trattamento dei dati personali è l'A.O.Pg che agisce attraverso il Direttore Generale, suo rappresentate legale, adottando tutte le misure tecniche ed organizzative atte a

garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali di riferimento aziendale sia effettuato conformemente alla normativa vigente.

Nel caso in cui l'A.O.Pg determini congiuntamente ad un altro o più Titolari del trattamento le finalità e i mezzi del trattamento, assume assieme a questi la veste di Contitolare del trattamento.

In tale ipotesi, i Contitolari determinano in modo trasparente, mediante un accordo interno scritto, le rispettive responsabilità in merito all'osservanza degli obblighi previsti dalla normativa vigente, con particolare riguardo all'esercizio dei diritti dell'interessato.

L'accordo suddetto specifica i rispettivi ruoli e i rapporti dei Contitolari con gli Interessati, che possono conoscerne il contenuto e esercitare i propri diritti nei confronti di e contro ciascun Titolare del trattamento.

Il Titolare, avvalendosi se del caso del Responsabile per la protezione dei dati, provvede a:

a) richiedere al Garante per la privacy l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
b) nominare i Responsabili designati e 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, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
c) nominare il Responsabile per la protezione dei dati, come stabilito dall'articolo 37 del Regolamento UE;
d) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
e) mettere in atto le misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente ai principi del Regolamento UE;
f) adottare il Documento Aziendale di Valutazione dei Rischi;
g) attivare e mantenere aggiornato, tramite i Responsabili interni del trattamento, il Registro delle attività di trattamento dei dati personali effettuati nell'A.O.Pg;
h) assicurare l'informazione e la formazione del personale sul tema della tutela della riservatezza dei dati personali.

ART. 18 - REPONSABILI ESTERNI DEL TRATTAMENTO E SUB-RESPONSABILI

L'A.O.Pg designa Responsabili esterni del trattamento dei dati personali, anche per mezzo dei Responsabili interni, per le rispettive competenze, tutti i soggetti esterni cui sono delegate attività di competenza aziendale o attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comunque comportano necessariamente il trattamento dei dati personali.

L'A.O.Pg designa quali Responsabili esterni del trattamento dei dati personali esclusivamente i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato.

Il Responsabile del trattamento dei dati personali non può delegare anche soltanto una parte dei trattamenti di dati personali che gli sono stati affidati ad altri soggetti, denominati Sub-Responsabili del trattamento, senza la previa e specifica autorizzazione scritta dell'A.O.Pg.

L'A.O.Pg disciplina le attività di trattamento dei dati personali affidate ai soggetti esterni con un apposito contratto (Allegato n.1), che vincola il Responsabile e l'eventuale Sub-Responsabile al Titolare del trattamento dei dati personali, in particolar modo per quanto riguarda la durata, la natura e la finalità del trattamento, il tipo di dati personali trattati, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

A tal fine le strutture aziendali, secondo le rispettive competenze, predispongono l'atto di nomina a Responsabile del trattamento, allegandolo se del caso alla deliberazione con la quale si approva lo schema contrattuale o di convenzione. L'atto di nomina sarà perfezionato contestualmente alla sottoscrizione del contratto o della convenzione. La sottoscrizione dell'atto di nomina e l'impegno a rispettare le disposizioni della normativa di settore è condizione essenziale per l'inizio dello specifico rapporto giuridico tra le parti.

Le strutture aziendali competenti per la gestione del contratto o della convenzione devono provvedere all'applicazione di quanto disciplinato nel presente Regolamento, adeguando, se necessario, anche mediante apposito atto aggiuntivo, i contratti o le convenzioni in essere ai sensi del presente Regolamento e della normativa vigente.

Nei contratti di affidamento di attività o di servizi all'esterno dell'Azienda è inserita un'apposita clausola di garanzia con cui il soggetto affidatario, individuato Responsabile del trattamento dei dati, si impegna, nel trattamento dei dati personali effettuati in forza del rapporto contrattuale, all'osservanza delle norme vigenti in materia di privacy e di quanto disposto dall'Azienda. Inoltre, qualora tra le attività oggetto del contratto o della convenzione rientrino le funzioni proprie dei cd. amministratori di sistema, di cui al provvedimento del Garante del 27/11/2008, la suddetta clausola deve essere integrata con la previsione di un impegno del seguente contenuto: *"il responsabile esterno del trattamento dei dati si impegna*

ad osservare le disposizioni del Garante in materia di Amministratori di Sistema conservando direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema fornendo il relativo elenco al Titolare". Rientra nella figura di amministratore di sistema il soggetto professionale dedicato alla gestione e alla manutenzione di impianti di elaborazione con i quali vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza nella misura in cui consentano di intervenire sui dati personali.

Il Responsabile del trattamento, in particolare, deve essere vincolato a:

a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa in materia di privacy;
b) trattare i dati personali, anche di natura sensibile e giudiziaria, dei pazienti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con l'Azienda e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
c) rispettare i principi in materia di sicurezza dettati dalla normativa vigente in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
d) adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento UE;
e) nominare, al proprio interno, i soggetti autorizzati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
f) attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a), del Regolamento UE;
g) specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati, su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati;
h) assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del

Regolamento UE (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

i) su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;

j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento UE e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Il Responsabile del trattamento risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli artt. 1218 e 1223 del Codice Civile.

Nel caso in cui un Responsabile del trattamento ricorra, previa specifica autorizzazione, a un Sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'A.O.Pg, a tale altro Sub-Responsabile del trattamento sono imposti, mediante un contratto, gli stessi obblighi a cui è stato sottoposto il Responsabile.

Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti dell'A.O.Pg l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile.

ART. 19 – RESPONSABILI INTERNI AL TRATTAMENTO DEI DATI PERSONALI

L'A.O.Pg designa i Responsabili Interni dei dati personali cui delegare il coordinamento delle attività di trattamento dei dati.

I Responsabili interni sono designati dal Titolare con apposito atto formale (allegato n. 2) accompagnato da specifiche indicazioni operative per il corretto assolvimento dei compiti a questi assegnati in materia di protezione dei dati.

L'A.O.Pg designa i Responsabili interni tra coloro che ricoprono gli incarichi di:

a) Direttore Amministrativo pro-tempore, per i trattamenti afferenti alle Direzioni dell'area amministrativa di linea, con le relative articolazioni, e le Direzioni o uffici di staff;

b) Direttore Sanitario pro-tempore per i trattamenti afferenti alle Direzioni di area sanitaria di linea, con le relative articolazioni, e le Direzioni o uffici di staff;

c) Direttore di Dipartimento;
d) Direttore/Responsabile delle strutture complesse e semplici dipartimentali, dell'area amministrativa, sanitaria, tecnica e professionale
e) IFO – Incarichi di Funzione Organizzativa

Sono designati altresì Responsabili Interni i Responsabili degli studi clinici ed osservazionali limitatamente ai trattamenti che da tale attività derivano.

La nomina del Responsabile Interno è effettuata con atto predisposto dal Titolare ed indica i trattamenti di dati dei quali viene conferita la responsabilità del coordinamento.

La S.C. Affari Generali e la S.C. Risorse Umane provvederanno, in ogni atto futuro, successivo all'adozione del presente Regolamento, avente ad oggetto il conferimento rispettivamente degli incarichi di cui alla lett. a), b) e c) (S.C. Affari Generali) e di cui alla lett. d) ed e) (S.C. Risorse Umane) sopra indicate, ad inserire nel contratto di lavoro la nomina di Responsabile interno dei dati personali da sottoscrivere da parte dell'interessato unitamente al contratto di incarico.

Per coloro che, alla data di adozione del presente Regolamento, ricoprono già gli incarichi di cui sopra, la nomina quale Responsabile Interno dei dati personali s'intende formalizzata con la sottoscrizione della delega al trattamento dei dati personali (allegato n. 2) operata dalla S.C. Affari Generali, conservato agli atti della Struttura e trasmesso al fascicolo personale per la conservazione.

Il Titolare può, inoltre, individuare quali Responsabili designati del trattamento altri soggetti (titolari di incarichi ecc.) in virtù delle particolarità organizzative e funzionali delle attività di competenza.

I Responsabili designati al trattamento dei dati personali si attengono agli obblighi individuati dalla normativa vigente e dal presente Regolamento e, più specificatamente, ai compiti e alle istruzioni contenuti nella nomina effettuata dal Titolare.

In particolare il Responsabile designato al trattamento deve:

a) trattare i dati personali osservando le disposizioni di legge e regolamentari, nonché le specifiche istruzioni impartite dal Titolare;
b) individuare nell'ambito del personale assegnato al proprio Servizio e secondo le modalità operative individuate le persone fisiche autorizzate al trattamento dei dati e darne comunicazione alla S.C. Risorse Umane, per la relativa autorizzazione e successiva attribuzione delle credenziali di identificazione da parte della S.C. Servizio Informatico;

c) individuare l'ambito di operatività assegnato a ciascun autorizzato, secondo quanto indicato nel provvedimento di nomina;

d) garantire che, presso il proprio Servizio, le persone autorizzate al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza e rispettino le istruzioni impartite loro mediante il provvedimento di nomina;

e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso il proprio Servizio, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;

f) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

g) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente;

h) contribuire alle attività di verifica del rispetto degli obblighi in materia, comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questi incaricato;

i) verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, nonché i profili di autorizzazione degli autorizzati al trattamento dei dati, rispondano ai principi di necessità, pertinenza, minimizzazione, sicurezza e legittimità;

j) verificare che all'interessato o al soggetto presso il quale sono raccolti i dati sia data l'informativa;

k) verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;

l) fornire al Responsabile per la protezione dei dati (RPD-DPO) e al Referente per il Trattamento dei dati personali ogni informazione e notizia rilevante ai fini degli obblighi in materia;

m) ottemperare ad ogni altro adempimento stabilito dal Titolare in relazione al trattamento dei dati personali;

n) collaborare con il Referente per il Trattamento dei dati personali e con il Referente informatico per la protezione dei dati nell'espletamento dei rispettivi compiti

o) aggiornare tempestivamente il registro dei trattamenti all'inizio di ogni nuovo trattamento, alla cessazione o alla modifica dei trattamenti in atto, condividendo altresì ogni notizia rilevante ai fini della tutela della sicurezza e riservatezza dei dati personali;

p) individuare in base a competenza e procedura aziendale i Responsabili Esterni del Trattamento utilizzando il modello adottato a sistema, vale a dire il fac simile allegato al presente atto sub 4 o quello generato dalla piattaforma gestionale in uso, non appena implementato;

q) segnalare ai Referenti ed al Responsabile per la protezione dei dati (RPD- D.P.O) i casi in cui a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare la perdita, la distruzione o la diffusione indebita di dati personali trattati nel rispetto dei provvedimenti del Garante (c.d. data breach).

I Responsabili designati al trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla vigente normativa in materia di privacy e dalle istruzioni ricevute, ivi comprese quelle riguardanti l'adozione delle misure di sicurezza.

La funzione di Responsabile designato al trattamento non è a sua volta delegabile. In caso di assenza o impedimento del Responsabile designato al trattamento, le relative attribuzioni sono esercitate da chi lo sostituisce per le attività di istituto.

Il personale del comparto incaricato del trattamento dei dati, che svolge attività di supporto all'esercizio dell'attività libero professionale intramuraria del personale dirigenziale, potrà procedere al trattamento dei dati secondo le specifiche autorizzazioni già in possesso per lo svolgimento delle attività istituzionali.

ART. 20 – AUTORIZZATI AL TRATTAMENTO

Gli autorizzati del trattamento dei dati personali sono le persone fisiche che effettuano le operazioni di trattamento di dati personali e/o particolari (sensibili), autorizzate, a tale scopo, dal Titolare del Trattamento.

Sono da designare come Autorizzati sia i dipendenti dell'A.O.Pg che i collaboratori i quali, a qualsiasi titolo (ad esempio: tirocinanti, studenti, stagisti, liberi professionisti, borsisti, consulenti), prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Azienda.

La loro designazione deve prevedere la trascrizione della data di inizio e eventuale fine dell'attività all'interno della struttura ed indicare i trattamenti di dati per i quali sono autorizzati a svolgere le relative operazioni.

Gli Autorizzati ricevono formale atto di autorizzazione al trattamento dal Titolare del Trattamento, che impartisce loro disposizioni sul corretto uso dei dati, in special modo sotto il

profilo della sicurezza e vengono informati sulle direttive vigenti sulla protezione dei dati da loro trattati (Allegato n. 3).

L'atto di cui sopra costituisce l'unico presupposto di liceità per il trattamento dei dati personali; l'originale di tale atto, controfirmato dallo stesso autorizzato, è conservato a cura del Titolare del trattamento ed una copia viene consegnata all'autorizzato.

La S.C. Risorse Umane provvederà, dall'adozione del presente Regolamento, a predisporre il contratto di lavoro o di incarico del restante personale diverso da quello di cui all'art. 19, mediante l'inserimento di un'apposita clausola che specifichi l'individuazione del soggetto quale Autorizzato al trattamento dei dati in relazione alle funzioni di competenza derivanti dal rapporto giuridico esistente con l'Azienda; inoltre, nelle more della definizione di un sistema automatizzato, metterà a disposizione della S.C. Servizio informatico le informazioni giuridiche ed organizzative comprensive di eventuali spostamenti interni, cessazione o altra variazione del predetto rapporto giuridico, che incida sulla figura di Autorizzato, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati.

Per coloro che, alla data di entrata in vigore del presente Regolamento, risultano avere già in atto un rapporto giuridico con l'Azienda, l'individuazione, quale Autorizzato al trattamento dei dati s'intende formalizzata, nelle more della definizione di un sistema automatizzato, con la pubblicazione del presente Regolamento nel sito web aziendale nell'apposita sezione intranet ed internet, al fine di darne massima conoscibilità a tutto il personale.

La designazione ad Autorizzato del trattamento dei dati personali non è direttamente collegata allo stato di dipendenza del personale o alla dipendenza funzionale del personale stesso dal Titolare che autorizza al trattamento.

Gli Autorizzati hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali di propria competenza.

Durante il trattamento od in caso di allontanamento dal posto di lavoro, l'Autorizzato deve adottare le misure previste e a propria disposizione, secondo le istruzioni ricevute dal Titolare, per evitare l'accesso non autorizzato da parte di terzi, anche se dipendenti, ai dati personali trattati o in trattamento.

Anche gli Autorizzati del trattamento che non sono tenuti per legge al segreto professionale sono sottoposti a regole di condotta analoghe al segreto professionale e all'assunzione di comportamenti metodologicamente corretti in materia di riservatezza e di protezione dei dati.

Inoltre, gli Autorizzati del trattamento dei dati personali:

- trattano i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza;

- qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata ed è fatto loro assoluto divieto di cedere la propria password ad altri;
- sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento e hanno l'obbligo di restituirli al termine delle operazioni affidate.

Sono altresì da designare Autorizzati i dipendenti e i collaboratori del Responsabile o Sub-Responsabile esterno del trattamento che, a qualsiasi titolo, prestino la loro opera, anche in via temporanea, trattando dati per conto dell'A.O.Pg.

In tale ultima ipotesi, tali Responsabili del trattamento conservano presso la loro sede legale gli originali degli atti di designazione ad Autorizzato.

ART.21 – OBBLIGHI DELLE PERSONE CHE OPERANO ALL'INTERNO DELL'AZIENDA

Tutte le persone che funzionalmente svolgono operazioni di trattamento su dati di cui l'A.O.Pg ha la titolarità, nonché prestano attività all'interno dell'A.O.Pg stessa a qualsiasi titolo, con o senza retribuzione, compresi gli allievi e i docenti dei corsi di formazione e di aggiornamento professionale, anche in convenzione con le università, gli specializzandi, i tirocinanti e i volontari, qualora in occasione della loro attività vengano a conoscenza di dati personali trattati dall'A.O.Pg sono autorizzati dai competenti Responsabili designati del trattamento quali autorizzati del trattamento dei dati ed assumono gli stessi obblighi degli autorizzati del trattamento.

Per le finalità del presente articolo il Responsabile del trattamento fornisce le necessarie informazioni alle persone che operano a qualsiasi titolo nella propria struttura.

ART. 22 – AMMINISTRATORI DI SISTEMA

L'A.O.Pg designa i propri Amministratori di Sistema, ai sensi del Provvedimento del Garante 27 novembre del 2008, come pubblicato in G.U. il 24 dicembre 2008, con apposito atto (Allegato n.4), corredato di specifiche istruzioni operative, e impartisce le opportune disposizioni perché sia assicurata l'effettività di tutte le misure ed audit previste dalla normativa vigente in tema di Amministratore di Sistema.

Gli Amministratori di Sistema sono tenuti al rilascio agli Autorizzati del trattamento delle credenziali per accedere alle procedure informatiche previa richiesta sottoscritta dal Responsabile interno.

Per quanto riguarda eventuali soggetti esterni cui si deleghino competenze di gestione e protezione dei sistemi informativi e delle risorse hardware e software dell'A.O.Pg, deve essere stipulato, con gli stessi, un atto giuridico con il quale sono designati Responsabili del trattamento dei dati, assegnando loro le specifiche funzioni di "Amministratore di Sistema" (tenuti, quindi, ad assolvere a tutte le misure ed audit previste dalla normativa vigente in tema di Amministratore di Sistema) elencando in maniera esaustiva tutte le attività che dovranno essere svolte.

ART. 23 – RESPONSABILE PER LA PROTEZIONE DEI DATI - RPD

L'A.O.Pg designa il Responsabile della Protezione dei Dati - RPD (o Data Protection Officer – DPO), individuandolo esclusivamente in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi aziendali in materia di protezione dei dati e della capacità di assolvere ai compiti individuati dalla normativa vigente.

L'A.O.Pg ne pubblica i dati di contatto e li comunica all'Autorità Garante Privacy, in conformità alle indicazioni da questa impartite.

Secondo l'art. 39 del GDPR, paragrafo 1, vengono assegnati al Responsabile per la Protezione dei Dati "almeno" i seguenti incarichi:

a) attività di informazione e consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, sugli obblighi derivanti dal regolamento e da altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati;
b) sorveglianza sull'osservanza, da parte del titolare o del responsabile del trattamento, del regolamento e delle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati, compresa l'attribuzione delle responsabilità, sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere sulla "valutazione d'impatto" della protezione dei dati e sorvegliarne l'adempimento ai sensi dell'art. 35 del GDPR;
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 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

La circostanza che la norma specifichi che il Responsabile per la Protezione dei Dati deve svolgere "almeno" questi compiti significa che nulla impedisce al Titolare del trattamento di assegnargli compiti ulteriori rispetto a quelli espressamente elencati nel paragrafo 1, oppure di specificare ulteriormente i compiti suddetti.

È evidente, pertanto, che, a parte la competenza sul regolamento europeo (dal punto di vista normativo e tecnico), il Responsabile per la Protezione dei Dati non ha una funzione operativa ovvero non è il soggetto che deve occuparsi degli adempimenti legati al trattamento dei dati all'interno dell'organizzazione ma è un soggetto di garanzia che deve verificare che l'organizzazione adotti dei processi, delle regole conformi a quelli che sono gli adempimenti voluti dal regolamento. L'attività svolta dal Responsabile per la Protezione dei Dati è prettamente consulenziale, di controllo e di audit, allo scopo di indirizzare al meglio le scelte del Titolare del trattamento, oltre che predisporre le privacy policy più adeguate al contesto di riferimento.

Il Titolare o il Responsabile interno del trattamento possono essere assistiti dal Responsabile per la Protezione dei Dati "nel controllo del rispetto a livello interno del presente regolamento". Secondo le Linee Guida del Gruppo di Lavoro art. 29[(1)] (punto 4.1) fanno parte di questi "compiti di controllo" svolti dal Responsabile per la Protezione dei Dati, in particolare:

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità;
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

ART. 24 – GRUPPO DI COORDINAMENTO AZIENDALE PER LA PROTEZIONE DEI DATI - GCPD

L'A.O.Pg, al fine di poter adempiere a tutte le complesse attività correlate alla materia della protezione dei dati personali, per sua natura necessariamente trasversale all'organizzazione aziendale, istituisce il Gruppo di Coordinamento per la Protezione dei Dati (GCPD) composto da:

- un Referente della S.C. Affari Generali;
- un Referente della S.C. Servizio Informatico;
- un Referente della S.C. Direzione Medica;
- un Referente della S.C. Servizio Infermieristico Tecnico Riabilitativo e Ostetrico (S.I.T.R.O.);
- un Referente della S.C. Economato;
- un Referente della S.C. Risorse Umane.

---

1 Linee Guida sui Responsabili della Protezione dei Dati (RPD) del Gruppo di Lavoro art. 29 in materia di protezione dei dati personali.

Al GCPD, che potrà essere integrato da altri Referenti in ragione della trattazione di materie specifiche, spettano le funzioni di:

- supportare il Responsabile per la Protezione dei Dati nello svolgimento delle sue funzioni;
- supportare il Titolare del trattamento nelle attività connesse al trattamento dei dati, compresa la tenuta del Registro dei Trattamenti, nella valutazione di impatto sulla protezione dei dati (DPIA);
- informare il Titolare di eventuali criticità fornendo supporto e cooperazione nel superamento della problematica;
- informare e sensibilizzare il personale dipendente riguardo agli obblighi derivanti dal Regolamento e da altre disposizioni in materia di protezione dati;
- sorvegliare l'osservanza in Azienda del Regolamento, valutando i rischi di ogni trattamento. Questi rischi devono anche essere rappresentati in modo corretto in tutta la documentazione che il Responsabile per la Protezione dei Dati deve "presidiare" e controllare;
- effettuare approfondimenti sulla materia, anche alla luce di successivi chiarimenti ed interpretazioni da parte delle autorità competenti, e aggiornarsi costantemente sulle evoluzioni della normativa.

Altri compiti affidati al GCPD potranno riguardare, a titolo esemplificativo, le seguenti attività aziendali:

- acquisti di beni e servizi di carattere strumentale: per essi occorre la valutazione del rispetto dei canoni della privacy by design e della privacy by default;
- obblighi formativi e informativi del personale;
- sicurezza reti e sistemi, ovvero adottare procedure e strumenti per la minimizzazione dei rischi di violazione dei dati per effetto della violazione della sicurezza; predisporre sistemi di minimizzazione dei danni come conseguenza di attacchi alla sicurezza;
- controlli e audit, ovvero inserire conformità al GDPR tra i parametri delle ispezioni interne;
- reclami e contenzioso, ovvero adottare procedure di gestione delle richieste di esercizio dei diritti e dei giudizi per risarcimento dei danni per violazione della riservatezza individuale.

ART. 25 – INFORMATIVA ALL'INTERESSATO

L'A.O.Pg adotta un sistema di documenti relativi alle informazioni sul trattamento dei dati personali chiare e comprensibili all'utenza per fornire all'interessato tutte le notizie relative al trattamento in forma coincisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Le informazioni sul trattamento dei dati personali riportano:

- l'identità e i dati di contatto del Titolare del trattamento e i dati di contatto del Responsabile per la Protezione dei Dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le modalità di trattamento dei dati personali;
- obbligatorietà o meno del conferimento dei dati;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- come possono essere esercitati i diritti di accesso in base alle disposizioni vigenti;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica del trattamento che lo riguarda o di opporsi al loro trattamento;
- qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio di consenso al trattamento il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di produrre reclamo al Garante per la protezione dei dati personali;
- se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure è un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, le indicazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
- nel caso in cui i dati personali non siano stati ottenuti presso l'interessato a questi deve essere resa nota la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Le informazioni all'interessato sono rese anche per estratto tramite l'affissione di appositi manifesti, o la somministrazione di appositi documenti, nei locali di accesso all'utenza, secondo procedure e modelli predisposti dal Titolare del trattamento.

L'A.O.Pg attiva, utilizzando diversi canali di comunicazione quali e-mail, sito aziendale, adeguate modalità di visibilità delle azioni poste in essere all'interno dell'Azienda in attuazione della normativa sulla riservatezza dei dati.

ART. 26 – DIRITTI DELL'INTERESSATO

Gli Interessati possono contattare il Titolare o il Responsabile della Protezione dei Dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

L'Interessato ha il diritto di ottenere dall'A.O.Pg la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali, laddove consentita, o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo al Garante per la protezione dei dati personali;
g) qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento.

L'interessato ha il diritto di ottenere dall'A.O.Pg la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

L'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'A.O.Pg si astiene dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgano sugli interessi, diritti e

libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, l'interessato ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

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

Se tali diritti sono riferiti a dati personali concernenti persone decedute, possono essere esercitati da chiunque vi abbia un interesse proprio o agisca a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

ART. 27 – INFORMAZIONI SULLO STATO DI SALUTE DELL'INTERESSATO

I dati personali inerenti la salute possono essere comunicati all'Interessato, o a soggetto da questi autorizzato, solo dal personale sanitario, in relazione alle specifiche competenze.

Le informazioni sullo stato di salute dei degenti sono fornite esclusivamente al degente stesso o a persona da questo formalmente designata.

A tal fine l'A.O.Pg ha adottato appositi moduli dei quali l'originale viene conservato in cartella clinica.

Per gli Interessati di minore età, le informazioni sullo stato di salute vengono fornite a chi esercita la responsabilità genitoriale.

In caso di impossibilità fisica, incapacità di intendere o di volere dell'interessato, le informazioni sul suo stato di salute sono fornite a chi ne esercita legalmente la potestà, al soggetto incaricato dall'autorità giudiziaria, ovvero ad un prossimo congiunto, un familiare, un convivente o, in loro assenza, al responsabile della struttura presso cui l'interessato dimora previa formale autocertificazione o dichiarazione delle suddette qualità.

ART. 28 – TRATTAMENTO DEI DATI PERSONALI TRA LE STRUTTURE DELL'AZIENDA

Il trattamento di dati personali effettuato all'interno dell'azienda per l'espletamento delle finalità istituzionali, dovrà essere effettuato soltanto nei limiti del principio di necessità, osservando le disposizioni del presente regolamento e delle relative misure di sicurezza.

ART. 29 – PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Il Titolare del trattamento mette in atto misure tecniche e organizzative volte ad attuare i principi di protezione dei dati in modo efficace e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento (che consentono, quindi, una *compliance* al Regolamento) e tutelare i diritti degli interessati sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso.

L'architettura di un Trattamento di dati personali deve essere configurata occupandosi della loro protezione fin dalla sua progettazione (privacy by design) e predisporre la protezione come condizione operativa automatica, per impostazione predefinita (privacy by default).

Il principio di Privacy by design ha lo scopo di garantire l'esistenza di un corretto livello di privacy e protezione dei dati personali fin dalla fase di progettazione e per tutto il ciclo di vita del trattamento. Il Titolare ed il Responsabile del Trattamento dovranno essere proattivi e preventivi, valutando e disponendo misure tecnico-organizzative per integrare nel trattamento le garanzie per la tutela dell'interessato e ad applicare i principi fondamentali della protezione di dati, quali trasparenza, limitazione delle finalità e minimizzazione. La pianificazione di un nuovo trattamento, dunque, deve partire da un'attività di valutazione d'impatto, quindi sull'anticipazione degli impatti potenziali, sulla delineazione di misure opportune di protezione, sulla progettazione di interventi meno onerosi e più efficaci e sull'integrazione e compatibilità con i processi esistenti.

In merito a quest'ultimo punto, risulta necessario effettuare un riesame dell'intero processo prima delle modifiche, prestando particolare attenzione ai servizi cruciali, e pianificare la revisione dell'intero processo.

Aderiscono al principio della Privacy by design misure tecnologiche di sicurezza, di protezione, come la pseudonimizzazione e cifratura dei dati, procedurali, come la riduzione al minimo del trattamento dei dati personali, ovvero consentire all'interessato di controllare il trattamento dei dati.

I processi delineati utilizzando il criterio della Privacy by design dovranno essere documentati e gestiti in modo tale da poter essere ricostruiti, dimostrando quali sono state le scelte effettuate per arrivare a raccogliere o meno determinate informazioni.

Il principio della Privacy by default garantisce che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento e per il periodo strettamente necessario, garantendo, inoltre, la non eccessività di tutti i dati raccolti. Ciò vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione

e l'accessibilità. Un trattamento dei dati personali così strutturato è una conseguenza della corretta progettazione del sistema nel suo complesso.

ART. 30 – VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (VIP) E CONSULTAZIONE PREVENTIVA CON IL GARANTE

Al Titolare del trattamento incombe, in forza dell'art. 35 del GDPR, paragrafo 1, di condurre una "Valutazione d'Impatto sulla Protezione dei dati" - VIP (o Data Protecion Impact Assessment – DPIA). Il ruolo del Responsabile per la Protezione dei Dati è però ugualmente significativo; infatti, in ossequio al principio di "privacy by design" (protezione dei dati fin dalla fase di progettazione), sancito nell'art. 35, paragrafo 2 del GDPR, il titolare "si consulta" con il Responsabile per la Protezione dei Dati quando svolge una "valutazione di impatto". Inoltre, ai sensi della lettera c) del paragrafo 1, dell'art. 39 del GDPR, il Responsabile per la Protezione dei Dati fornisce, "se richiesto", un "parere" in merito alla "valutazione di impatto" e ne sorveglia l'adempimento ai sensi dell'art. 35 del GDPR.

In particolare le Linee Guida, punto 4.2 (Gruppo di Lavoro art. 29) raccomandano che il Titolare si consulti con il Responsabile per la Protezione dei Dati, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre una DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al Regolamento.

Qualora il Titolare non concordi con le indicazioni fornite dal Responsabile per la Protezione Dati, è necessario, per le Linee Guida, che la documentazione relativa alla DPIA riporti le motivazioni per cui si è ritenuto non conformarsi a tali indicazioni.

Il Responsabile per la Protezione dei Dati, come prescritto dal paragrafo 2 dell'art. 39 del GDPR, deve considerare, nell'esecuzione dei propri compiti, i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. È una disposizione con la quale si chiede al Responsabile per la Protezione dei Dati di definire un ordine di priorità nell'attività svolta e di rivolgere un'attenzione prioritaria alle questioni che presentino i rischi più elevati in termini di protezione dei dati. Ciò al fine di essere più facilmente in grado di consigliare al Titolare quale metodologia seguire nello

svolgere una DPIA, a quali settori riservare un audit in termini di protezione dei dati, quali attività di formazione interna prevedere per il personale o amministratori che trattino dati personali e a quali trattamenti dedicare maggiori risorse e tempo.

ART. 31 – MISURE DI SICUREZZA

Il Titolare del trattamento e i Responsabili designati al trattamento dei dati (Interni ed esterni) sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, tenuto conto:

- dello stato dell'arte e dei costi di attuazione;
- della natura, del campo di applicazione, del contesto e delle finalità del trattamento;
- del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (risultati della valutazione di impatto DPIA).

Tali misure comprendono:

- la pseudonimizzazione, trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive (sempre che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire la non attribuzione a una persona identificata o identificabile);
- la cifratura;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si deve tener conto dei rischi presentati da trattamenti di dati derivanti:

- dalla distruzione, perdita e modifica;
- dalla divulgazione non autorizzata;
- dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati.

Il Titolare del trattamento e i Responsabili designati al trattamento fanno sì che chiunque agisca sotto la loro autorità ed abbia accesso a dati personali, tratti tali dati solo se istruito in tal senso dal Titolare del trattamento.

Chiunque ha il diritto di non essere sottoposto a una misura, che produca effetti giuridici o che significativamente incida sulla sua persona, basata unicamente su un trattamento automatizzato, destinato a valutare taluni aspetti della sua personalità o ad analizzarne o prevederne in particolare il rendimento professionale, la situazione economica, l'ubicazione, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento (profilazione).

Se i dati sono trattati in base a contratto o con il consenso dell'interessato, o nel rispetto di una disposizione di legge, devono essere chiaramente previste e indicate le garanzie a tutela dei suoi legittimi interessi.

Il trattamento automatizzato di dati personali destinato a valutare taluni aspetti della personalità dell'interessato non può basarsi unicamente sulle categorie particolari di dati personali sensibili.

L'accesso ad ogni procedura informatica è consentito solo se congruente con il trattamento di dati per il quale il collaboratore dell'A.O.Pg è stato precedentemente designato Autorizzato al trattamento ed è consentito soltanto utilizzando apposite credenziali personali composte da un user-id, attribuito dall'Amministratore di Sistema di competenza e da una password.

La password è strettamente personale e, a nessun titolo, può essere comunicata a terzi. Della sua riservatezza risponde personalmente il singolo incaricato del trattamento dei dati personali.

ART. 32 – MISURE DI SICUREZZA PER I TRATTAMENTI DI DATI PERSONALI AFFIDATI A SOGGETTI ESTERNI

I Responsabili e Sub-Responsabili esterni del trattamento sono tenuti ad assicurare al Titolare del trattamento di aver adottato, prima di effettuare attività di trattamento di dati, ogni misura di sicurezza prevista dalla normativa vigente in tema di protezione di dati e amministrazione digitale.

Tali soggetti sono comunque tenuti a:

a) assicurare il rispetto delle specifiche istruzioni operative impartite dall'Azienda per la tenuta in sicurezza dei dati oggetto di affidamento e di aver ulteriormente attivato ogni altra misura idonea alla protezione dei dati loro affidati;
b) comunicare all'Azienda le procedure adottate per la sicurezza dei dati con riferimento, tra l'altro, a:
    - l'attività svolta e le misure di sicurezza adottate;

- l'elenco degli autorizzati del trattamento e l'indicazione della sede presso la quale le relative autorizzazioni sono custodite;
- l'elenco delle risorse hardware e software;
- le procedure di continuità operativa ed emergenza adottate;
- le misure di eventuale recupero da disastro adottate;
- le misure adottate di back-up degli specifici sistemi informativi aziendali utilizzati per i trattamenti autorizzati, di contenimento dei virus / malware informatici, e altre misure, comprese quelle di eventuale conservazione sostitutiva;
- le eventuali criticità che potrebbero costituire occasione di accesso non consentito o perdita / manomissione del patrimonio informativo gestito per conto dell'Azienda;
- le misure adottate per la cifratura o la separazione dei dati relativi alla salute;
- le misure adottate per la gestione delle disposizioni in tema di amministratori di sistema;
- le verifiche periodiche sul mantenimento in sicurezza che sono state adottate, con la relativa documentazione.

Il mancato rispetto da parte del Responsabile del trattamento dell'adozione delle misure di sicurezza adeguate a prevenire o contenere i rischi che possono riguardare i dati oggetto dell'affidamento può costituire titolo per la risoluzione per giusta causa del rapporto sottostante e per chiedere il risarcimento dei danni subiti.

ART. 33 – INTERVENTI TECNICI A CURA DI SOGGETTI ESTERNI

I soggetti esterni che, in forza di un rapporto contrattuale con l'Azienda, esercitino attività di manutenzione su apparecchiature utilizzate per il trattamento o la registrazione di dati, sono nominati Amministratori di Sistema e devono fornire idonea garanzia del rispetto delle misure di sicurezza previste dalla normativa vigente.

Nel caso in cui sia necessario un intervento tecnico su apparecchiature contenenti dati personali o che comunque ne permettono il trattamento da parte di soggetti esterni non vincolati all'A.O.Pg da un preesistente rapporto contrattuale, il direttore della struttura aziendale competente a commissionare la specifica manutenzione è tenuto a far vigilare da parte degli Autorizzati del trattamento l'operato degli esecutori del servizio per la durata del servizio stesso.

Preliminarmente alla stipula di ogni nuovo contratto di manutenzione, il direttore della struttura aziendale competente provvede a richiedere al soggetto esterno le garanzie previste dal Regolamento, dando altresì indicazione delle specifiche esigenze di sicurezza dell'Azienda.

ART.34 – TENUTA IN SICUREZZA DEI DOCUMENTI E DEGLI ARCHIVI

Gli archivi che custodiscono i dati di cui è titolare del trattamento l'A.O.Pg, cartacei e digitali, devono essere collocati in locali non esposti a rischi ambientali in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo aziendale in tema di Continuità Operativa, Conservazione Sostitutiva e Disaster Recovery (DR o Recupero dal Disastro – RD).

La documentazione archiviata, anche digitalmente, che riporta dati personali è conservata per il tempo previsto dalla legge e poi sottoposta a scarto di archivio o cancellata definitivamente.

Il Responsabile del trattamento attiva, attenendosi alle disposizioni e Procedure Aziendali vigenti, i meccanismi necessari a garantire l'accesso controllato ai locali e l'accesso selezionato ai dati mediante registrazione degli accessi.

I supporti contenenti dati personali diversi dal cartaceo (supporti informatici, magnetici, videoregistrazioni effettuate nell'ambito dell'attività clinica, bobine di microfilm, immagini iconografiche), debbono essere conservati e custoditi con le modalità indicate per gli archivi cartacei, se non diversamente stabilito, nei modi e termini previsti dalla normativa vigente.

L'accesso agli archivi cartacei aziendali è formalmente autorizzato da parte dei Responsabili designati al trattamento.

Relativamente agli archivi digitali, il rilascio di tale autorizzazione è di competenza dell'Amministratore di Sistema, previa indicazione del competente Responsabile interno.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Responsabile designato al trattamento dei dati di competenza, che deve assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.

Per quanto riguarda la documentazione cartacea facente parte dell'archivio aziendale storico e/o di deposito, in conformità a quanto disposto dal Ministero per i Beni Culturali ed Ambientali con l'apposito Massimario di scarto per gli archivi degli Enti Sanitari, periodicamente l'A.O.Pg predispone un piano di scarto d'archivio, approvato con apposita deliberazione.

Relativamente agli archivi informatizzati di dati l'A.O.Pg adotta, facendo seguito alle disposizioni vigenti in tema di protezione dati e amministrazione digitale, idonee procedure di:

- salvataggio periodico degli archivi di dati personali;
- misure di contenimento dei virus / malware informatici e di protezione perimetrale da cyber attacchi alle infrastrutture ICT aziendali;
- *disaster recovery*;
- continuità operativa;

- conservazione sostitutiva.

Resta obbligatorio segnalare eventuali criticità e problematiche al Titolare ed al Responsabile per la Protezione dei Dati.

ART. 35 – LIMITI ALLA CONSERVAZIONE DEI DATI PERSONALI

L'A.O.Pg assicura l'adozione di apposite misure e procedure attraverso le quali:

- si proceda alla distruzione dei documenti analogici e digitali, una volta terminato il limite minimo di conservazione dei documenti e dei dati in questi riportati;
- siano smaltiti gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l'A.O.Pg;
- il riutilizzo di apparati di memoria o hardware sia effettuato con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è titolare l'A.O.Pg.

ART. 36 – ATTIVITA' DI VERIFICA E DI CONTROLLO DEI TRATTAMENTI DI DATI PERSONALI

L'A.O.Pg individua modalità attraverso cui si svolgono le attività di verifica e controllo, anche periodico, del rispetto delle misure di legge e delle ulteriori disposizioni impartite durante le operazioni di trattamento dei dati da parte dei Responsabili designati, Sub-Responsabili, Amministratori di Sistema e Autorizzati del trattamento.

I controlli e le verifiche sono effettuati previa programmazione periodica o, in caso di necessità, anche su sollecitazione degli interessati, e le relative attività sono svolte dal personale a ciò incaricato sotto il coordinamento del Responsabile per la Protezione dei Dati.

ART. 37 – FORMAZIONE DEI RESPONSABILI DESIGNATI, AUTORIZZATI E AMMINISTRATORI DI SISTEMA

L'A.O.Pg, inserisce nel proprio Piano Annuale di Formazione iniziative atte ad assicurare la formazione e il continuo aggiornamento dei Responsabili designati al trattamento, degli Autorizzati da questi coordinati, degli Amministratori di Sistema e del personale di nuova assunzione sui temi della protezione dei dati personali e sui diritti, doveri ed adempimenti previsti dalla normativa vigente.

Per il personale di nuova assunzione, l'obbligo formativo, almeno in fase iniziale, potrà eventualmente essere soddisfatto attraverso la messa a disposizione di specifica documentazione all'uopo predisposta.

I Responsabili ed i Sub-Responsabili esterni del trattamento sono tenuti a assicurare all'A.O.Pg che gli Autorizzati e gli Amministratori di Sistema che svolgono attività di trattamento di dati personali su loro mandato, siano formati e continuamente aggiornati. Inoltre di tale formazione dovrà essere data evidenza, su richiesta, al Titolare del trattamento.

ART. 38 – VIOLAZIONE DEI DATI PERSONALI

Ogni Responsabile designato o Autorizzato al trattamento dei dati personali è tenuto a informare, senza ingiustificato ritardo, il Titolare ed il Responsabile della Protezione Dati del possibile caso di una violazione dei dati personali (*Data Breach*).

In tali casi, l'A.O.Pg avvia le necessarie procedure e, avvalendosi della collaborazione dei Responsabili designati del trattamento accerta lo stato dell'arte.

Il Titolare dell'A.O.Pg provvede a notificare, con il supporto del Responsabile per la Protezione dei Dati, la violazione all'Autorità Garante Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli Interessati.

Qualora la notifica non sia effettuata entro le 72 ore, questa è corredata dei motivi del ritardo.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati, a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente.

Tale comunicazione non deve essere fatta se:

- sono attuate protezioni tecniche e organizzative (dati incomprensibili o cifrati);
- sono attuati provvedimenti ulteriori che annullano di fatto i rischi per i diritti e la libertà dell'interessato;
- la notifica comporta uno sforzo sproporzionato, maggiore dell'adozione di misure alternative ugualmente efficaci.

Quindi, diventa importante la misura di sicurezza, perché il fatto che la violazione possa generare danni rilevanti a interessati dipende anche dal livello di sicurezza e dalle misure di sicurezza adottate nel senso che, se il Titolare/Responsabile del trattamento adotta, per esempio, dei sistemi di pseudonimizzazione e/o cifratura, i danni che possono derivare nei confronti degli interessati potrebbero essere notevolmente ridotti. Al contrario, l'accesso da parte del soggetto responsabile della violazione a dati in chiaro, potrebbe accrescere notevolmente i rischi connessi ad una violazione.

La notifica al Garante della violazione dei dati personali deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del Responsabile per la Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali in un apposito registro delle violazioni di dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione consente all'autorità di controllo di verificare il rispetto delle indicazioni di legge.

ART. 39 – DISCIPLINA DELLE MISURE DEL REGOLAMENTO

L'A.O.Pg provvede ad adottare procedure, Disciplinari, Linee Guida e Indicazioni Operative e Regolamenti di settore che consentano l'applicazione del presente Regolamento e delle misure di legge a protezione dei dati personali.

L'A.O.Pg persegue nella protezione dei dati personali il continuo miglioramento qualitativo, attraverso l'emanazione di specifici provvedimenti e procedure, nonché attraverso la formulazione e l'aggiornamento di linee guida operative e comportamentali.

ART. 40 – NORME FINALI E DI RINVIO

L'A.O.Pg si riserva di adeguare, modificare o integrare il testo del presente regolamento per motivi organizzativi e/o normativi e qualora le direttive sopra citate lo rendano opportuno.

Per tutto quanto non espressamente previsto dal presente regolamento, si applica la normativa vigente in tema di protezione dei dati personali e amministrazione digitale.

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 del medesimo.

ART. 41 – ENTRATA IN VIGORE

Il presente Regolamento entrerà in vigore a partire dal giorno successivo alla data di pubblicazione dello stesso sul sito aziendale "Amministrazione Trasparente", sezione "Regolamenti".

Con effetto dalla data di entrata in vigore del presente Regolamento cessa l'efficacia delle precedenti disposizioni Regolamentari in materia.

GLOSSARIO

Di seguito un breve glossario dei termini utilizzati nel presente regolamento.

Archivio

Qualsiasi insieme strutturato di dati, anche personali, accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Autorità di controllo

Autorità pubblica indipendente individuata nel Garante per la protezione dei dati personali.

L'autorità istituita dalla legge 31 dicembre 1996, n. 675 che rappresenta l'attuazione, a livello nazionale, di quanto previsto dall'articolo 51 del GDPR, deputata alla sorveglianza dell'applicazione del regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche coinvolte nel trattamento di dati personali, nonché di agevolare la libera circolazione dei dati personali all'interno dell'Unione Europea.

Autorità Giudiziaria

Autorità giurisdizionale competente.

Autorizzati

Persone fisiche autorizzate a compiere operazioni di trattamento sotto la diretta autorità del Titolare e/o Responsabile interno al trattamento.

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli autorizzati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Consenso dell'Interessato

Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, affinché i dati che lo riguardano siano oggetto di trattamento.

Credenziali di autenticazione

Consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave.

Dati Biometrici

I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati Genetici

I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati Giudiziari

I dati personali idonei a rilevare provvedimenti 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.

Dati identificativi

I dati personali che permettono l'identificazione diretta dell'interessato.

Dati Personali

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.

Dati relativi alla salute

I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute.

Dati appartenenti alle categorie particolari

I dati personali idonei a rilevare 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.

I dati particolari, (già "dati sensibili") non possono essere diffusi ma possono essere oggetto di comunicazione, anche attraverso soggetti pubblici, solo se previsto da disposizioni di legge e/o di regolamento.

Dato Anonimo

il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Responsabile Interno del trattamento

La persona fisica con incarichi apicali all'interno della struttura, che tratta dati personali per conto del titolare del trattamento alla quale è affidato il coordinamento e la vigilanza delle operazioni di trattamento di dati personali effettuate dagli autorizzati.

Destinatario

La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Diffusione

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

Garante per la protezione dei dati personali

v. Autorità di controllo.

GDPR

Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Interessati

Persone fisiche a cui si riferiscono i dati personali oggetto del trattamento.

Limitazione di trattamento

Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Profilazione

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

Pseudonimizzazione

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'ausilio di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Registro dei Trattamenti

Il Registro delle attività di trattamento tenuto dal titolare in ottemperanza a quanto prescritto dall'articolo 30 del GDPR.

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".

Responsabile della Protezione dei Dati (RPD)

È una persona fisica o giuridica, nominata obbligatoriamente nei casi di cui all'art. 37 del Regolamento europeo n. 679/2016 dal Titolare o dal Responsabile del trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto del predetto Regolamento. Nel caso sia nominata una persona giuridica, deve essere comunque individuato un referente al suo interno.

Sub-responsabile

Soggetti terzi di cui il Responsabile esterno si avvale per l'esecuzione dei trattamenti di dati personali funzionali all'erogazione dei servizi oggetto del Contratto, previa autorizzazione del Titolare.

Terzo

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persona autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

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.

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.

Violazione dei dati personali

La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Allegato 1

ATTO DI NOMINA DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI AI SENSI DEGLI ART. 28 DEL REG. UE 2016/679 ("GDPR")

Il Sottoscritto Dott. xxxxxxxxxxxxxx, nella sua qualità di Dirigente della Struttura Complessa xxxxxxxxx e come tale Responsabile interno designato dalla Azienda Ospedaliera di Perugia (C.F. - P. IVA 02101050546), con sede legale in Perugia, Ente da qui in avanti indicato come "Titolare del Trattamento" dei dati personali,

- visto che l'Azienda Sanitaria di Perugia, in qualità di Titolare del Trattamento ai sensi dell'Art. 4, par. 1, n.° 7) dell'intestato Regolamento (c.d. "GDPR"), intende avvalersi della facoltà di nomina di responsabili esterni dei propri trattamenti ex art. 28 GDPR;

- vista la designazione a Responsabile interno, relativamente ai trattamenti effettuati all'interno della Struttura Complessa sopra indicata;

- visto che con la Ditta nominanda sussiste rapporto di fornitura come da XXXX n.° xxx del xxx, comportante trattamento di dati personali da effettuarsi per conto del Titolare del Trattamento, come meglio precisato nella successiva tabella;

- considerata la particolare natura del contratto e l'impatto che le attività di cui al suddetto contratto hanno sul trattamento dei dati personali e ritenuta opportuna e necessaria la nomina della suddetta Ditta a Responsabile Esterno del Trattamento;

ai sensi dell'Art. 28 del Reg. U.E. 2016/679

NOMINA

RESPONSABILE ESTERNO DEL TRATTAMENTO

la xxxxxx (C.F./P.IVA xxxxx), con sede in xxxx (xx) al civico n.° xx della Via xxxxxx (di seguito "Responsabile Esterno", o "Responsabile"), in persona del Legale Rappresentante *pro tempore*.

Con la sottoscrizione per ricevuta ed accettazione del presente atto, da considerarsi *addendum* contrattuale al rapporto già in essere tra le Parti, il Responsabile Esterno:

- accetta, a titolo gratuito, la nomina a Responsabile Esterno dei trattamenti dei dati personali di cui al richiamato contratto e meglio precisati nella seguente tabella:

N.	Descrizione Trattamento	Interessati	Tipologia dati	Finalità del trattamento	Modalità del trattamento
1	*(riga di esempio, da eliminare)*	*Pazienti del reparto xxxx*	*Anagrafici e sanitari*	*Istituzionali di cura e ricerca*	*Cartaceo e digitale*

2					
3					

- conferma la sua diretta nonché approfondita conoscenza degli obblighi che assume in relazione a quanto disposto dal Codice Privacy (D.Lgs. n. 196/2003 modificato dal D.Lgs. n. 101/2018) e dal GDPR e dichiara di essere in possesso dei requisiti e delle capacità sufficienti a garantire l'adozione di misure tecniche e organizzative adeguate, in modo tale che il trattamento dei dati personali e dei dati appartenenti alle categorie particolari soddisfi i requisiti del GDPR e garantisca la tutela dei diritti degli interessati (art. 28, par. 1 GDPR).

In qualità di Responsabile del trattamento, dovrà:

- osservare quanto disposto dalla vigente normativa in tema di protezione dei dati personali ed in particolare dal D. Lgs. 196/2003, dal Reg. UE 2016/679, dai provvedimenti del Garante della Privacy, dalle istruzioni impartite sia nel presente atto, sia in successive ed eventuali comunicazioni della Titolare del Trattamento (art. 28, par. 1 GDPR). Ove rilevi la propria impossibilità a rispettare tali istruzioni, anche a causa del caso fortuito o della forza maggiore (quali danneggiamenti, anomalie di funzionamento delle protezioni e controllo accessi, ecc.) sarà obbligato ad avvertire immediatamente la Titolare nonché adottare le possibili e più ragionevoli misure di tutela dei dati;
- comunicare alla Titolare del trattamento l'elenco di tutti gli eventuali soggetti che svolgano, per conto del Responsabile medesimo, il ruolo di "Sub-Responsabili" per la cui nomina si fornisce espressa autorizzazione scritta generale. La Titolare del trattamento potrà verificare eventuali profili di criticità emergenti dalle comunicazioni ricevute e si riserva la facoltà di limitare e/o revocare l'autorizzazione generale qui concessa. Nel caso in cui nel tempo intervengano modifiche, aggiunte o sostituzioni dei sub-responsabili inizialmente comunicati, tali nuove nomine dovranno essere inoltrate alla Titolare del trattamento al fine di effettuare le opportune valutazioni (anche in termini oppositivi) relativamente alla protezione dei dati personali. Il

Responsabile del trattamento deve individuare e nominare in forma scritta i propri sub-responsabili. L'atto di nomina/individuazione dovrà riproporre a carico del Sub-Responsabile i medesimi obblighi posti a carico del Responsabile e specificati nel presente documento; in particolare l'atto dovrà individuare le misure tecniche ed organizzative adeguate per garantire che il trattamento soddisfi i requisiti di sicurezza richiesti dalla Legge e dall'Allegato III delle Clausole contrattuali tipo di cui alla Decisione di esecuzione (EU) n. 915/2021 del 4 giugno 2021 in tutti gli asset del Sub-Responsabile interessati dal trattamento dei dati personali previsti dal Contratto. Qualora i Sub-Responsabili del trattamento omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserverà, nei confronti della Titolare del trattamento, l'intera responsabilità dell'adempimento degli obblighi dei Sub-Responsabili (art. 28, par. 4 GDPR);

- trattare i dati soltanto su istruzione documentata della Titolare del Trattamento, anche in caso di trasferimento dei dati personali verso un Paese terzo o un'Organizzazione internazionale, salvo che lo richieda il diritto dell'UE o nazionale cui risulta essere soggetto il Responsabile del trattamento. In tal caso il medesimo dovrà informare la Titolare del Trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico [art. 28, par. 3, lett. a) GDPR];
- individuare le persone che, sotto la propria autorità, eseguono materialmente le operazioni di trattamento sui dati personali per conto del Titolare e nominarle per iscritto "persone autorizzate al trattamento dei dati personali", nonché – se del caso – Amministratori di sistema, fornendo loro, sempre per iscritto, appropriate e complete istruzioni su come effettuare il trattamento, garantendo altresì che le persone autorizzate al trattamento si siano impegnate alla riservatezza o che abbiano un obbligo legale di riservatezza [art. 28, par. 3, lett. b) GDPR];
- adottare [art. 28, par. 3, lett. c) GDPR] le misure di sicurezza previste dall'art. 32 GDPR e ritenute idonee a garantire la riservatezza, l'integrità, la disponibilità e la custodia in ogni fase del trattamento dei dati (quali se del caso la pseudonimizzazione e la cifratura dei dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico...), tenendo conto sia della natura, della finalità del trattamento che dei rischi e facendo espresso riferimento alle Misure minime di sicurezza ICT per le Pubbliche Amministrazioni come da Circolare AGID 2017 e s.m.i.;
- tenere conto della natura del trattamento e assistere la Titolare del Trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo di

quest'ultima di dare seguito alle richieste per l'esercizio dei diritti dell'interessato previsti dagli artt. 12 – 23 GDPR [art. 28, par. 3, lett. e) GDPR];

- assistere la Titolare del Trattamento allo scopo di garantire il rispetto degli obblighi di cui agli artt. 32 – 36 GDPR ("Sicurezza dei dati personali"), tenendo conto della natura del trattamento e delle informazioni di cui dispone [art. 28, par. 3, lett. f) GDPR];
- cancellare o restituire, su scelta della Titolare del Trattamento, tutti i dati personali al termine della propria prestazione di servizio, e cancellare le copie esistenti, salvo che il diritto dell'Unione o quello nazionale preveda la conservazione di tali dati [art. 28, par. 3, lett. g) GDPR];
- mettere a disposizione della Titolare tutte le informazioni necessarie al fine di dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, nonché consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dalla Titolare del Trattamento o da altro soggetto da questa incaricato. Dovrà, inoltre, informare immediatamente la Titolare del Trattamento qualora, a suo parere, un'istruzione violi il GDPR o il Codice Privacy o altre disposizioni relative alla protezione dei dati [art. 28, par. 3, lett. h) GDPR];
- informare la Titolare del Trattamento, senza giustificato ritardo, di ogni violazione dei dati personali (art. 33, par. 2 GDPR) al fine di consentire alla Titolare stessa il rispetto delle attività di notifica all'Autorità di controllo. La comunicazione dovrà avvenire senza ingiustificato ritardo all'indirizzo PEC ufficiale e dovrà contenere informazioni circa: a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero almeno approssimativo di interessati in questione, nonché le categorie e il numero almeno approssimativo di registrazione dei dati personali in questione; b) il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni; c) la descrizione delle probabili conseguenze della violazione dei dati personali; d) la descrizione delle misure adottate da parte del Responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi. Il Responsabile sarà tenuto a mantenere presso i propri uffici la documentazione necessaria a descrivere le violazioni dei dati subite;
- tenere il Registro delle Attività di Trattamento dei dati, svolte sotto la propria responsabilità (art. 30 GDPR) ed esibirlo a richiesta dalla Titolare del Trattamento;
- cooperare con l'Autorità di controllo nell'esecuzione dei suoi compiti (art. 31 GDPR);
- trattare i dati nel rispetto dei principi di liceità, correttezza, trasparenza, legittimità, esattezza, aggiornamento, pertinenza, non eccedenza, completezza, adeguatezza e conservazione, limitatamente al conseguimento della finalità che il suo incarico

prevede e nell'osservanza di quanto disposto dagli artt. 1, 2-decies del nuovo Codice Privacy e 5 del GDPR (minimizzazione dei dati);

La presente nomina è condizionata, per oggetto, durata, natura e finalità del trattamento, nonché per il tipo di dati personali, per le categorie di interessati, per gli obblighi e i diritti della Titolare del trattamento al contratto di cui in premessa (in fase di esecuzione) e si intenderà revocata di diritto contestualmente alla cessazione o alla risoluzione dello stesso.

Perugia, lì_____

Dott. xxxxxxxxxx (n.q.) _____

Il Responsabile del trattamento_____

Allegato 2

NOMINA DEL RESPONSABILE INTERNO DEL TRATTAMENTO

Il Direttore Generale

Visto l'art. 4, par. 1, n. 8 del Reg. U.E. 2016/679;

In qualità di titolare del trattamento dei dati personali, nell'esercizio delle attribuzioni previste dagli artt. 4 par. 1, n. 7; 24 e 28 del Reg. U.E. 2016/679

NOMINA

il Dott. Xxxxxxxxxxxxxx, nella sua qualità di _____, quale Responsabile del Trattamento dei dati personali trattati all'interno del Servizio _____.

Il Responsabile procede al trattamento dei dati personali attenendosi alle istruzioni impartite dal Titolare, il quale, anche tramite visite periodiche, vigila sulla puntuale osservanza delle disposizioni e delle istruzioni impartite.

In particolare il Responsabile designato al trattamento deve:

a) trattare i dati personali osservando le disposizioni di legge e regolamentari, nonché le specifiche istruzioni impartite dal Titolare;
b) individuare nell'ambito del personale assegnato al proprio Servizio e secondo le modalità operative individuate le persone fisiche autorizzate al trattamento dei dati e darne comunicazione alla S.C. Risorse Umane, per la relativa autorizzazione e successiva attribuzione delle credenziali di identificazione da parte della S.C. Servizio Informatico;
c) individuare l'ambito di operatività assegnato a ciascun autorizzato, secondo quanto indicato nel provvedimento di nomina;
d) garantire che, presso il proprio Servizio, le persone autorizzate al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza e rispettino le istruzioni impartite loro mediante il provvedimento di nomina;
e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso il proprio Servizio, il rispetto dei diritti, delle libertà fondamentali e della

dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;

f) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

g) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente;

h) contribuire alle attività di verifica del rispetto degli obblighi in materia, comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questi incaricato;

i) verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, nonché i profili di autorizzazione degli autorizzati al trattamento dei dati, rispondano ai principi di necessità, pertinenza, minimizzazione, sicurezza e legittimità;

j) verificare che all'interessato o al soggetto presso il quale sono raccolti i dati sia data l'informativa;

k) verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;

l) fornire al Responsabile per la protezione dei dati (RPD-DPO) e al Referente per il Trattamento dei dati personali ogni informazione e notizia rilevante ai fini degli obblighi in materia;

m) ottemperare ad ogni altro adempimento stabilito dal Titolare in relazione al trattamento dei dati personali;

n) collaborare con il Referente per il Trattamento dei dati personali e con il Referente informatico per la protezione dei dati nell'espletamento dei rispettivi compiti;

o) aggiornare tempestivamente il registro dei trattamenti all'inizio di ogni nuovo trattamento, alla cessazione o alla modifica dei trattamenti in atto, condividendo altresì ogni notizia rilevante ai fini della tutela della sicurezza e riservatezza dei dati personali;

p) individuare in base a competenza e procedura aziendale i Responsabili Esterni del Trattamento utilizzando il modello adottato a sistema, vale a dire il fac simile allegato al presente atto sub 4 o quello generato dalla piattaforma gestionale in uso, non appena implementato;

q) segnalare ai Referenti ed al Responsabile per la protezione dei dati (RPD-D.P.O) i casi in cui a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare la perdita, la distruzione o la diffusione indebita di dati personali trattati nel rispetto dei provvedimenti del Garante (c.d. data breach).

E' consentito il ricorso alla delega scritta di funzioni da parte del designato, previa approvazione del Titolare.

Perugia, lì_____

Il Direttore Generale

_____

Sottoscrizione del Responsabile Interno del trattamento

_____

Allegato 3

LETTERA DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI ED EVENTUALI CATEGORIE PARTICOLARI

L'**AZIENDA OSPEDALIERA DI PERUGIA** (C.F. - P. IVA 02101050546), con sede legale in Perugia, in persona del Direttore Generale – legale rappresentante pro tempore, in qualità di Titolare del Trattamento dei dati personali, ai sensi dell'art. 2-quaterdecies del Codice della Privacy (D.Lgs. n. 196/03 come modificato dal D.Lgs. n. 101/2018) e dell'art. 29 del Regolamento U.E. 2016/679 (c.d. GDPR),

AUTORIZZA

il/la Sig./ra xxxxxxxxxxxxxxx xxxxxxxxxxxx, nato/a a xxxxxxxxxx il xxxxxx e residente in xxxxxxxx, Via xxxx n.° xxxxxx, dipendente (tirocinante/stagista...)

AL TRATTAMENTO DI DATI PERSONALI

ED EVENTUALI CATEGORIE PARTICOLARI

vale a dire, limitatamente alle mansioni previste per il suo inquadramento, l'incarico di curare 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 dei dati oggetto di trattamento da parte del Titolare del trattamento e relativi agli interessati, quali pazienti, utenti, fornitori e dipendenti.

L'autorizzato è tenuto ad operare, oltre che nel rispetto della normativa vigente, in base al Regolamento Interno ed alle Istruzioni fornite dal Titolare del trattamento, che con la sottoscrizione del presente atto dichiara di conoscere.

Perugia, lì_____

Dott. Giuseppe De Filippis (n.q.)

Sottoscrizione dell'Autorizzato al trattamento

_____

Allegato 4

NOMINA DI AMMINISTRATORE DI SISTEMA

L'Azienda Ospedaliera di Perugia, in persona del legale rappresentante pro tempore, in qualità di Titolare del trattamento dei dati ai sensi del Regolamento UE 2016/679,

- visto il Provvedimento del Garante per la Protezione dei dati personali del 27 novembre 2008 e successive modifiche, recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*";

- tenuto conto delle competenze possedute e del ruolo ricoperto nell'organizzazione aziendale della Società, dopo averne anche verificato l'idoneità rispetto alle caratteristiche di esperienza, capacità e affidabilità richieste dalle vigenti disposizioni per adempiere agli obblighi in materia di sicurezza del trattamento informatico dei dati e per svolgere attività di gestione tecnica del sistema informatico

NOMINA

il Sig. _____ nato a ..... il ....., residente a ..... codice fiscale ....., che opera nell'organizzazione aziendale in qualità di .....…, Amministratore di Sistema con i seguenti compiti:

1. prendere tutti i provvedimenti necessari ad evitare rischi per i dati – quali, a titolo esemplificativo e non esaustivo, accesso non autorizzato, perdita o distruzione - e provvedere al ricovero periodico degli stessi con copie di back-up secondo i criteri stabiliti dal Titolare/Responsabile del Trattamento dei dati;
2. assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
3. effettuare il trattamento dei dati personali in modo lecito e secondo correttezza, nel perseguimento di finalità determinate, esplicite e legittime, garantendone la riservatezza;
4. è fatto divieto procedere alla modifica, alla cancellazione, alla distruzione o alla perdita di dati nonché al compimento di qualsiasi operazione di trattamento che non sia espressamente autorizzata;
5. informare prontamente il Titolare di tutte le questioni rilevanti ai fini del rispetto della normativa soprarichiamata, in particolare di eventuali violazioni che dovessero

occorrere ai dati personali (c.d. data breach);

6. sovrintendere al buon funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
7. monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
8. effettuare interventi di aggiornamento e manutenzione hardware e software su sistemi operativi e applicativi;
9. sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;
10. generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli autorizzati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;
11. procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
12. gestire le password di root o di amministratore di sistema;
13. collaborare con il responsabile del trattamento dei dati personali e con il DPO;
14. verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi installati nei pc presenti nell'unità produttiva;
15. indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;
16. adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Della nomina ad Amministratore di sistema, così disposta con il presente atto, verrà data opportuna informazione nell'ambito dell'organizzazione aziendale della Società, ed al personale interessato, con le modalità più opportune.

Con la sottoscrizione del presente atto, l'Amministratore di sistema accetta la nomina,

conferma altresì la diretta ed approfondita conoscenza della normativa più volte citata nonché degli obblighi in essa prevista.

Il Titolare provvederà, con cadenza almeno annuale, a svolgere le dovute verifiche sulle attività compiute dall'Amministratore di sistema. È obbligo di quest'ultimo prestare alla Società la sua piena collaborazione per il compimento delle verifiche stesse; in ogni caso, è tenuto a predisporre, con cadenza semestrale, una relazione scritta delle attività svolte in esecuzione delle incombenze affidatigli in forza del presente atto.

Azienda Ospedaliera di Perugia_____

L'Amministratore di Sistema _____