AZIENDA SANITARIA PROVICIALE DI RAGUSA

REGOLAMENTO AZIENDALE
IN MATERIA DI PROTEZIONE DEI DATIPERSONALI

sulla base del

Regolamento Europeo 679/2016 del Parlamento europeo
e del Consiglio del 27 aprile 2016 ("GDPR")
e del d.lgs. 196/2003 e ss.mm.ii. ("Codice Privacy")

Data di emissione	**26 novembre 2018**	**Versione**	**1.0**
Data di revisione	**17 settembre 2024**	**Revisione**	**2.0**

Sommario

Premessa

Il presente Regolamento è stato predisposto per disciplinare, attraverso una serie di misure che compongono un vero e proprio "Sistema Gestionale Privacy", i compiti e le responsabilità di tutti coloro che trattano dati personali nell'ambito dell'Azienda Sanitaria Provinciale di Ragusa (di seguito "ASP").

Il Regolamento è stato elaborato tenendo conto dell'attuale quadro normativo, composto sia dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "GDPR"), sia dalle indicazioni del Decreto Legislativo n. 196 del 30 giugno 2003, così come adeguato dal D.lgs. n. 101 del 10 agosto 2018 e ss.mm.ii. (di seguito "Codice Privacy"), che costituiscono il basamento del sistema di accountability, adottato dall'ASP nella sua veste di Titolare del trattamento, che sarà opportunamente implementato con tutte le misure derivanti da questo Regolamento organizzativo.

Disposizioni di riferimento

- Decreto legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali" così come adeguato dal Decreto legislativo n. 101 del 10 agosto 2018 ss.mm.ii.;
- 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;
- Decreto Legislativo n. 82 del 7 marzo 2005 "Codice dell'Amministrazione digitale" e ss.mm.ii.;
- Legge n. 241 del 7 agosto 1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e ss.mm.ii.;
- Decreto legislativo n. 33 del 14 marzo 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 ss.mm.ii.;
- Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di Dossier sanitario del 16 luglio 2009, adottate dal Garante per la protezione dei dati personali;
- 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 del 28 maggio 2014, adottate dal Garante per la protezione dei dati personali;
- Linee guida in materia di Dossier sanitario del 4 giugno 2015, adottate dal Garante per la Protezione dei Dati Personali.

Glossario

a) **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno

o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) **«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;

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

d) **«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;

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

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

g) **«titolare del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

h) **«data protection officer o dpo»:** è una persona fisica, 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, a livello interno, del predetto Regolamento

i) **«delegato al trattamento»:** la persona fisica che tratta dati personali per conto del titolare del

trattamento alla quale è affidato il coordinamento e la vigilanza delle operazioni di trattamento dei dati personali effettuate dagli incaricati

j) **«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;

k) **«autorizzati/incaricati»**: persone fisiche autorizzate a compiere operazioni di trattamento sotto la diretta autorità del Titolare e/o del Responsabile del trattamento e/o del Delegato del trattamento;

l) **«Interessato»**: persona fisica cui si riferiscono i dati personali;

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

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

o) **«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;

p) **«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;

q) **«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;

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

s) **«Dati identificativi»**: i dati personali che permettono l'identificazione diretta dell'interessato;

t) **«Dati giudiziari»:** i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

u) **«Dati particolari»**: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale. I dati di salute non possono essere diffusi. I dati sensibili sono oggetto di comunicazione anche verso soggetti pubblici solo se prevista da disposizioni di legge o di regolamento;

v) **«Dato anonimo»**: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

w) **«Comunicazione»**: il dare conoscenza dei dati personali ad 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;

x) **«Garante per la Protezione dei Dati Personali o Garante»**: l'autorità pubblica indipendente deputata al controllo del rispetto della normativa vigente in materia di protezione dei dati personali.

Articolo 1 - Oggetto ed ambito di applicazione

Il presente Regolamento individua le politiche aziendali di ASP relative alla corretta gestione del trattamento dei dati personali, così come definiti dal GDPR, dal Codice Privacy e dai Provvedimenti del Garante per la Protezione dei Dati personali, attraverso l'individuazione di una serie di misure che compongono un vero e proprio "Sistema Gestionale Privacy", nonché dei compiti e delle responsabilità di tutti coloro che nell'ASP trattano dati personali.

Il documento è stato elaborato tenendo conto dell'attuale quadro normativo e contribuisce al miglioramento del sistema di accountability adottato dall'ASP, nella sua veste di Titolare del trattamento. L'ASP si impegna ad implementarlo attraverso l'attuazione di tutte le necessarie misure da questo derivanti.

Articolo 2 - I Principi

L'ASP, anche in considerazione dell'estrema delicatezza dei dati personali che correntemente tratta, della loro molteplicità e della numerosità dei soggetti che necessariamente concorrono al trattamento, 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 dei criteri di adeguatezza.

A riguardo, l'ASP 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:

- «liceità, correttezza e trasparenza», cioè siano trattati in modo lecito, corretto e trasparente nei confrontidell'interessato;
- «limitazione della finalità», cioè siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- «minimizzazione dei dati», cioè questi debbano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- «esattezza», cioè siano 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 della conservazione», cioè siano 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 richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;
- «integrità e riservatezza», cioè 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», cioè adottando e essendo in grado di dimostrare che il trattamento dei dati viene svolto nel pieno rispetto della normativa vigente.

Articolo 3 - L'accountability e il Sistema Gestionale Privacy dell'ASP

L'ASP mette in atto tutte le misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità del trattamento, in considerazione del possibile rischio di lesione dei diritti e delle libertà degli Interessati.

Tali misure sono riesaminate e aggiornate periodicamente e, negli ulteriori casi in cui ciò si renda necessario, vengono adottate politiche adeguate in materia di protezione dei dati.

Tali misure compongono il Sistema Gestionale Privacy aziendale, che include:

- l'Ufficio Privacy
- il Gruppo di lavoro Privacy;
- le altre Funzioni Privacy definite nel presente Regolamento;
- il Registro delle attività di trattamento dei dati;
- il sistema di attribuzione delle responsabilità del trattamento dei dati personali;
- la documentazione relativa alle informative ed al rilascio delle autorizzazioni al trattamento dei dati;
- la documentazione relativa alle valutazioni di impatto;
- le regolamentazioni, le policy, le procedure e le disposizioni operative adottate dall'ASP;

- l'analisi dei rischi e il relativo documento di valutazione;
- il sistema di audit e verifica periodica del corretto trattamento dei dati personali;
- il sistema di gestione delle violazioni dei dati personali;
- il sistema di formazione continua dei Delegati del trattamento, degli Autorizzati del trattamento e degli Amministratori di sistema.

L'ASP integra il Sistema Gestionale Privacy al fine di realizzare una struttura integrata in evoluzione continua, fondamentale per far sì che l'innovazione e la revisione organizzativa dei processi sanitari siano non solo un investimento fondamentale per migliorare il rapporto costo-qualità dei servizi sanitari, limitare sprechi e inefficienze, ridurre le differenze tra i territori, ma anche per migliorare la qualità percepita dal cittadino attraverso un percorso di crescita e maturazione del sistema ASP che possa coniugare efficacemente bisogni, opportunità ed effettivo rispetto dei diritti, in piena *compliance* con la normativa privacy vigente.

Articolo 4 - Categorie di Interessati e di dati personali trattati dall'Azienda

L 'ASP 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'ASP;
- clienti e fornitori;
- partecipanti a bandi, gare e selezioni;
- eventuali strutture partner.

I dati personali trattati comprendono anche le seguenti tipologie di dati particolari:
- dati idonei a rivelare lo stato di salute e la vita sessuale;
- dati soggetti a maggior tutela;
- dati genetici;
- dati biometrici.

Inoltre, l'ASP può trattare i dati relativi a condanne penali e reati: si tratta dei dati giudiziari, in quanto possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Ai sensi del GDPR, sono ricompresi in tale nozione anche i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Nei casi e con i limiti previsti dalle normative di settore vigenti, l'ASP, altresì, tratta dati personali particolari per la rilevazione delle malattie mentali, malattie infettive e diffusive, nonché della sieropositività, a fini di indagini epidemiologiche, a fini di trapianto di organi e tessuti, a fini di monitoraggio della spesa sanitaria; questi sono trattati qualora siano essenziali e necessari allo svolgimento delle attività istituzionali indicate dal precedente articolo 2 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'ASP nelle forme e nei limiti di quanto previsto dalla normativa vigente sono raccolti:

- direttamente e prioritariamente 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, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri, opresso altri esercenti professioni sanitarie.

Per effettuare il trattamento dei dati personali, l'ASP 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, quando previsto dalla normativa vigente, soltanto previa somministrazione 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.

Articolo 5 - Le finalità del trattamento dei dati personali

I trattamenti di dati personali effettuati dall'ASP 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.

Articolo 6 – Il consenso al trattamento dei dati personali

L'ASP tratta i dati personali idonei a rivelare lo stato di salute a fini di diagnosi, cura e riabilitazione, soltanto dopo avere erogato specifica informativa ai soggetti interessati.

Laddove la base giuridica sia individuabile esclusivamente nel consenso, il trattamento dei dati suindicati è effettuato, qualora la legge o i Provvedimenti dell'Autorità Garante per la Protezione di Dati personali dispongano in tal senso, previa acquisizione di specifico consenso da parte degli Interessati.

In tali casi, il Titolare assicura, attraverso idonee modalità, la corretta gestione e archiviazione di tali consensi in modo da renderli fruibili e rintracciabili, nonché per gestire le eventuali istanze di revoca che pervengano dagli Interessati.

Articolo 7 - Il trattamento dei dati personali

Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento dei dati e, per l'effetto, delle Funzioni Privacy dell'ASP previste nel presente Regolamento, nel rispetto delle disposizioni ivi previste.

All'interno dell'ASP 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'ASP.

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 (principio di minimizzazione).

I dati personali devono essere trattati dalle Funzioni privacy dell'ASP, in relazione al relativo ruolo, in modo lecito e sono raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni di trattamento in termini non incompatibili con tali scopi.

I Delegati del 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.

Le Funzioni Privacy dell'ASP sono autorizzate all'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento dei dati personali è consentito.

I Delegati sono tenuti a comunicare dati personali comuni e/o particolari agli altri Delegati del 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 Delegati e i Responsabili del trattamento 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 preconfigurati, in ossequio al già principio della "privacy per impostazione predefinita", riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, così da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare

l'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 del Garante.

Articolo 8 - Il trattamento dei dati particolari

L'ASP tratta dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o 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 fisicaqualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato allafinalità perseguita;
h) 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;
i) 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 deisistemi e servizi sanitari o sociali o conformemente al contratto con un professionista della sanità;
j) il trattamento è necessario per motivi di interesse 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;
k) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o afini statistici.

Qualora il trattamento sia basato sul consenso, è compito dell'ASP 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, 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 basato sul consenso ed effettuato prima della revoca.

Articolo 9 - Il controllo a distanza

Ad ogni sistema di controllo a distanza degli Interessati e/o del lavoratore, l'ASP applica il principio di proporzionalità tra mezzi impiegati e fini perseguiti, nel rispetto delle disposizioni vigenti e delle ulteriori direttive dell'Autorità Garante per la Protezione dei Dati personali.

L'ASP comunque garantisce il rispetto della disciplina del divieto di controllo a distanza del lavoratore, così come prevista dalla normativa di riferimento, nonché degli accordi con le rappresentanze sindacali aziendali, adottando i conseguenti regolamenti applicativi.

Per tutti i sistemi di controllo attivati dall'ASP, 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.

Articolo 10 - Il Registro delle attività di trattamento dei dati personali

L'ASP 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'ASP 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'ASP tiene un Registro informatico delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato a cura dei Delegati e dell'Ufficio Privacy, che evidenzia i diversi livelli di responsabilità attribuiti in relazione al trattamento dei dati, suddivisi per Delegati, Autorizzati ed Amministratori di Sistema e contiene le seguenti informazioni:

1. i trattamenti che vengono svolti;
2. per ognuno di questi, i Delegati, gli Autorizzati del trattamento e gli Amministratori di Sistema di riferimento;
3. il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento e del Data Protection Officer;
4. le finalità del trattamento;
5. una descrizione delle categorie di interessati e delle categorie di dati personali trattati;

6. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
7. gli eventuali trasferimenti di dati personali verso un paese terzo e la documentazione delle garanzie adeguate;
8. i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
9. una descrizione generale delle misure di sicurezza tecniche e organizzative adottate per proteggere i dati personali oggetto di trattamento.

Tale Registro viene tenuto anche dai Responsabili e Sub-Responsabili del trattamento.

Il Registro è tenuto in formato elettronico e, su richiesta, viene messo a disposizione del Garante.

Articolo 11 - Il Titolare del trattamento dei dati personali

Il Titolare del trattamento dei dati personali è l'ASP (di seguito anche "Titolare"). Tale soggetto, che agisce attraverso il Direttore Generale, suo rappresentante legale, adotta tutte le misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare nel rispetto del principio di *accountability*, che il trattamento dei dati personali svolto dall'ASP è effettuato conformemente alla normativa vigente in materia di protezione dei dati personali.

Nel caso in cui l'ASP 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 ai sensi dell'art. 26 del GDPR. 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 in materia di protezione dei dati personali, con particolare riguardo all'esercizio dei diritti degli interessati, nonché le rispettive responsabilità di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Il contenuto essenziale dell'accordo sarà messo a disposizione degli Interessati.

Il Titolare, con il supporto dei ruoli privacy di volta in volta competenti, come meglio specificato agli articoli seguenti del presente Regolamento, provvede, nei casi previsti dalla normativa applicabile in materia di protezione dei dati personali:

a) ad assolvere ogni obbligo di comunicazione, interpello o notificazione, verso l'Autorità Garante per la Protezione dei dati personali;
b) a cooperare, su richiesta, con l'Autorità nell'esecuzione dei suoi compiti;
c) a richiedere all'Autorità ogni necessaria autorizzazione preventiva al trattamento dei dati personali, ovenecessario;
d) ad adottare, per quanto di competenza e in relazione alle caratteristiche di ciascun trattamento posto in essere, le misure tecniche e organizzative adeguate necessarie a garantire la sicurezza delle operazioni di trattamento;
e) a designare il Data Protection Officer, dotandolo di necessarie e adeguate risorse;
f) ad adottare il Documento Aziendale di Valutazione dei Rischi;

g) ad attivare e mantenere aggiornato il Registro delle attività di trattamento dei dati personali effettuatida ASP, sia come Titolare sia come Responsabile;
h) ad assicurare l'informazione e la formazione del personale sul tema della tutela della riservatezza e della protezione dei dati personali;
i) a nominare, in conformità al Modello Organizzativo di ultima approvazione, i ruoli privacy ivi previsti;
j) a nominare i soggetti esterni che trattano dati personali per conto di ASP quali Responsabili del trattamento o Sub-Responsabili del trattamento di dati personali, impartendo loro le necessarie istruzioni per la corretta gestione e protezione dei dati personali, in conformità alle prescrizioni contenute nell'art. 28 del GDPR. Il Titolare, in base alle disposizioni vigenti in materia di protezione dei dati, effettuerà nei confronti di tutti i Responsabili del trattamento nominati verifiche e ispezioni volti a monitorare il rispetto degli obblighi impartiti.

Articolo 12 - I Responsabili del trattamento dei dati personali e i Sub-Responsabili

L'ASP nomina Responsabili del trattamento dei dati personali (di seguito anche "Responsabili") tutti i soggetti esterni tenuti a svolgere attività di competenza aziendale o attività connesse, strumentali e di supporto, ivi incluse le attivitàmanutentive, che comportano necessariamente il trattamento dei dati personali per conto del Titolare.

L'ASP designa quali Responsabili esclusivamente i soggetti che presentano garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'interessato.

Senza preventiva e specifica autorizzazione scritta dell'ASP, il Responsabile non può delegare, anche soltanto in parte, i trattamenti di dati personali che gli sono stati affidati dal Titolare ad altri soggetti, denominati Sub-Responsabili del trattamento (di seguito anche "Sub-Responsabili").
Nel caso in cui un Responsabile ricorra, previa specifica autorizzazione dell'ASP, a un Sub- Responsabile per l'esecuzione di specifiche attività di trattamento, a tale Sub-Responsabile sono imposti, mediante un contratto, gli stessi obblighi a cui è stato sottoposto il Responsabile. Qualora il Sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti dell'ASP l'intera responsabilità per l'inadempimento del Sub-Responsabile.

L'ASP disciplina le attività di trattamento dei dati personali affidate ai Responsabili con un apposito contratto o altro atto giuridico avente forma scritta, predisposto dall'Ufficio Privacy, che vincola il Responsabile e l'eventuale Sub-Responsabile, qualora autorizzato, al rispetto degli obblighi e delle istruzioni impartite dal Titolare (in particolar modo, riguardanti la durata, la natura e la finalità del trattamento, il tipo di dati personali oggetto di trattamento, le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento, etc.).

L'atto di designazione a Responsabile, anche quando realizzato in formato elettronico, prevede che il Responsabile:

a) tratti i dati personali per conto del Titolare nel rispetto delle istruzioni dallo stesso impartite e debitamente documentate;
b) vincoli gli Autorizzati del trattamento dei dati personali a mantenere la riservatezza sui trattamenti agli stessi affidati;
c) adotti tutte le misure di sicurezza indicate dall'ASP e le ulteriori misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, natura, oggetto, contesto e finalità del trattamento, rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
d) collabori con l'ASP al fine di dare seguito alle richieste di esercizio dei diritti degli interessati e garantire il rispetto degli obblighi di legge, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
e) su indicazione dell'ASP, cancelli o restituisca alla stessa i dati personali trattati per suo conto una volta terminata la prestazione dei servizi contrattualmente definita e ne cancelli le copie esistenti;
f) metta a disposizione dell'ASP le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuisca alle attività di controllo, revisione e ispezioni realizzati dal Titolare o da un altro soggetto da questi incaricato.

In tutti gli atti giuridici che disciplinano i rapporti con i Responsabili (contratti, convenzioni, scritture private, conferimenti d'incarico, etc.), deve inoltre essere inserita l'indicazione che l'ASP provvederà a designare il contraente quale Responsabile, con apposito atto separato contenente specifiche istruzioni operative, da formalizzare prima che abbia inizio l'attività di trattamento dei dati esercitata per conto del Titolare.

Tutte le strutture interne all'ASP che provvedono alla stesura o validazione degli atti con cui sono delegate a soggetti esterni attività di competenza aziendale o attività connesse, strumentali e di supporto, ivi incluse le attivitàmanutentive, che comunque comportano necessariamente il trattamento dei dati personali per conto del Titolare, sono tenute a segnalare l'affidamento *in itinere* all'Ufficio Privacy, che provvederà a predisporre l'apposita documentazione.

Articolo 13 - I Delegati al trattamento dei dati personali

L'ASP designa formalmente, attraverso apposito atto, Delegati al trattamento dei dati personali (di seguito anche "Delegati"), i soggetti tenuti al coordinamento delle attività di trattamento dei dati nell'ambito di una specifica area. L'atto di designazione viene notificato a ciascun Delegato per iscritto e contiene specifiche istruzioni il cui rispetto garantisce il corretto assolvimento dei compiti assegnati in materia di protezione dei dati.

L'ASP individua quali Delegati esclusivamente i soggetti che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti degli interessati.
In particolare, in continuità con la delibera n. 1140 del 12 giugno 2018, l'ASP designa come Delegati i

soggetti che ricoprono i seguenti incarichi:

- Direttore Amministrativo *pro-tempore,* per i trattamenti afferenti agli uffici di Segreteria Generalee Amministrativa e i relativi uffici di staff;
- Direttore Sanitario *pro-tempore*, per i trattamenti afferenti agli uffici della Segreteria di riferimento,nonché alle unità operative dell'area di staff della direzione medesima;
- Direttore/Responsabile delle unità operative complesse e semplici, dell'area amministrativa, sanitaria, tecnica e professionale;
- Direttore di Dipartimento strutturale, nonché i Responsabili delle unità operative complesse e semplici afferenti detto dipartimento;
- Direttore di Distretto Sanitario;
- Direttore di Presidio Ospedaliero.

Sono designati, altresì, quali Delegati:

- i dipendenti che svolgono attività libero- professionale *intra-moenia*;
- i responsabili degli studi clinici e osservazionali limitatamente ai trattamenti che da tale attivitàderivano.

La Direzione Risorse Umane, deputata alla gestione del personale e delle attività *intra-moenia*, nonché il Funzionario deputato alla gestione degli studi clinici ed osservazionali, sono tenuti a trasmettere tempestivamente all'Ufficio Privacy ogni informazione relativa all'inserimento o sostituzione, nell'ambito aziendale, di soggetti che ricoprono i ruoli sopra citati, affinché tale Ufficio possa predisporre gli atti necessari alla designazione dei Delegati.

L'atto di designazione dei Delegati è predisposto dall'Ufficio Privacy e indica i trattamenti di dati rispetto ai quali viene conferita a ciascun Delegato la responsabilità del relativo coordinamento.

Il Titolare, tramite l'Ufficio Privacy, conserva l'originale degli atti di designazione sottoscritti dai Delegati, nonché l'elenco dei Delegati nominati dall'ASP.

I Delegati si attengono agli obblighi individuati dalla normativa vigente in materia di protezione dei dati e dal presente Regolamento e, più specificamente, ai compiti e alle istruzioni impartiti come descritti nel relativo atto di designazione.

La funzione di Delegato è attribuita personalmente e non è suscettibile di delega.

I Delegati:

- non possono trattare i dati personali se non sono previamente istruiti in tal senso dall'ASP;
- mettono a disposizione dell'ASP tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuiscono alle attività di revisione, comprese le ispezioni, da questa realizzate;
- informano immediatamente l'Ufficio Privacy qualora un'istruzione ricevuta violi il presente Regolamento o altre disposizioni vigenti relative alla protezione dei dati personali, inviando un'apposita comunicazione all'indirizzo mail dedicato.

I Delegati compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza, sicurezza e protezione dei dati relativamente ai trattamenti loro assegnati e, in particolare, hanno il dovere di osservare e far osservare, all'interno dell'area di propria competenza:

- le misure di sicurezza e le altre precauzioni individuate nel Documento di Analisi e Valutazione dei Rischi adottato dall'ASP;
- le disposizioni relative alle misure di sicurezza adottate dall'ASP, alla modalità del trattamento dei dati, alla riservatezza e all'amministrazione digitale.

I Delegati sono dotati di autonomia gestionale e organizzativa per il trattamento dei dati di propria competenza e sono tenuti, inoltre, ad adottare ogni misura necessaria per il rispetto della riservatezza nell'erogazione delle prestazioni e dei servizi sanitari.

È compito dei Delegati verificare che la documentazione e le procedure che supportano l'attività di trattamento dei dati di propria competenza rispondano ai principi di necessità, pertinenza e non eccedenza, segnalando all'Ufficio Privacy eventuali situazioni di potenziale compromissione della protezione dei dati personali.

I Delegati, relativamente al proprio settore di competenza, rispondono verso il Titolare per ogni violazione o mancato adempimento di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale e riferiscono periodicamente al Titolare, per il tramite dell'Ufficio Privacy, su come svolgono i compiti specifici loro assegnati e, se esistente, segnalano ogni problematica correlata non appena di loro conoscenza.

I Delegati designano formalmente i soggetti Autorizzati o designati al trattamento (di seguito anche "Autorizzati"), fornendo loro per iscritto istruzioni operative dettagliate e specifiche sulle corrette modalità di trattamento dei dati personali svolti nell'ambito delle mansioni loro affidate. I Delegati, altresì, vigilano sul rispetto di tali istruzioni da parte degli Autorizzati, anche attraverso verifiche periodiche.

L'ASP riconosce a ciascun Delegato la possibilità di individuare e nominare, tra gli Autorizzati dell'area di competenza, un incaricato alla gestione privacy, quale figura di supporto nella gestione dell'operatività e degli adempimenti data protection.

Articolo 14 - Gli Autorizzati al trattamento dei dati personali e l'incaricato alla gestione privacy

Gli Autorizzati sono le persone fisiche che effettuano le operazioni di trattamento di dati personali (anche appartenenti alle categorie particolari), su incarico e previa designazione da parte del Delegato o del Responsabile. Con riferimento a questo secondo caso, vengono Autorizzati-Designati i dipendenti e i collaboratori del Responsabile o Sub-Responsabile che, a qualsiasi titolo, prestino la loro opera, anche in via temporanea, in favore di ASP, trattando dati personali per conto della stessa. In tale ipotesi, i Responsabili/Sub-Responsabili conservano presso la loro sede gli originali degli atti di nomina ad Autorizzato e su richiesta ne inviano copia via mail all'Ufficio Privacy.

All'interno dell'ASP vengono designati come Autorizzati sia i dipendenti che i collaboratori aziendali che, a qualsiasi titolo (ad esempio personale distaccato, tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti), prestino la loro opera, anche in via temporanea, all'interno delle strutture del Titolare.

Per la loro designazione è utilizzata apposita modulistica, predisposta dall'Ufficio Privacy, che contiene i riferimenti alla data di inizio - ed eventuale fine - dell'attività lavorativa all'interno della struttura del Titolare, nonché ai trattamenti di dati che gli Autorizzati possono svolgere nell'ambito delle mansioni svolte.

Gli Autorizzati sono formalmente designati dal Delegato che presiede l'area di assegnazione e – dunque – ove svolgono le attività di trattamento dei dati personali, il quale impartisce loro specifiche istruzioni sulle modalità di trattamento dei dati, anche sotto il profilo della sicurezza, nonché li informa sulle disposizioni vigenti sulla protezione dei dati da loro trattati.

L'atto di designazione ad Autorizzato costituisce presupposto di liceità per il trattamento dei dati personali da parte del soggetto designato; tale atto può essere firmato utilizzando due modalità alternative: con firma autografa e la sua scansione inserita nel registro dei trattamenti, oppure in modalità informatica. In quest'ultimo caso, il file di tale atto è sottoscritto informaticamente (firma debole) per presa visione dallo stesso Autorizzato e i dati (compreso il documento) sono in automatico rilevati nel Registro delle attività di trattamento del Titolare. Il Delegato e l'Ufficio Privacy in ogni caso hanno evidenza dei riferimenti e delle evidenze dell'avvenuta firma all'interno del Registro delle attività di trattamento del Titolare. L'Autorizzato o il Delegato cura la conservazione del documento in file.

L'evidenza dell'atto di nomina ad Autorizzato può essere stampata o salvata in pdf dallo stesso che lo conserva, tutti i riferimenti sono registrati all'interno del registro dei trattamenti, interrogabile dall'Ufficio Privacy e dal Delegato della UO, che è tenuto a controllare e aggiornare le date di cessazione dell'incarico affinché ne sia dato atto all'interno del Registro delle attività di trattamento del Titolare.

La designazione ad Autorizzato non è direttamente collegata allo stato di dipendenza del personale o alla dipendenza funzionale del personale stesso da parte del Delegato che autorizza il trattamento.

Gli Autorizzati, tra i diversi compiti loro affidati

a. trattano i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza;
b. 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;
c. 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.

Tra gli Autorizzati dell'area di competenza, il Delegato può individuare e nominare un incaricato alla gestione privacy, quale supporto per la gestione delle attività e degli adempimenti data protection. Sotto tale profilo detto incaricato ha, perciò, gli stessi diritti operativi del Delegato e pertanto può inviare le nomine ai nuovi autorizzati.

Articolo 15 - Gli Amministratori di sistema

L'ASP designa i propri Amministratori di sistema con apposito atto, il cui originale viene conservato presso l'Ufficio Privacy e caricato sul registro dei trattamenti, corredato di specifiche istruzioni operative e impartisce le opportune disposizioni perché sia assicurata l'effettività di tutte le misure e adempimenti previsti dal Provvedimento generale dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento dell'Autorità Garante per la protezione dei dati personali del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità compatibile con il GDPR.

Gli Amministratori di sistema rilasciano agli Autorizzati le credenziali per accedere sistemi informatici, previa richiesta sottoscritta dal Delegato di riferimento.
Gli stessi sono tenuti, inoltre, a inoltrare le richieste suindicate all'Ufficio Privacy, che le conserva assieme agli atti di nomina ad Autorizzato, verificandone la congruità.

Per quanto riguarda i Responsabili e Sub-Responsabili cuisono state delegate competenze di gestione e protezione dei sistemi informativi e delle risorse hardware e software dell'ASP, a questi viene impartito l'onere di designare e coordinare l'attività degli Amministratori di Sistema e presidiare tutti gli adempimenti in materia previsti dalla normativa vigente e dai già citati Provvedimenti del Garante per la protezione dei dati personali, compreso il rispetto delle misure di controllo dell'attività. Tali Responsabili e Sub-Responsabili sono pertanto tenuti ad assolvere a tutte le misure e adempimenti previsti dalla normativa vigente in tema di Amministratore di Sistema e a trasmettere al Titolare sia l'evidenza delle nomine implementate sia delle ulteriori misure adottate sia- copia della relativa documentazione, il tutto entro il mese di gennaio di ogni anno solare.
Infine, i Responsabili e Sub-Responsabili del trattamento sono tenuti a trasmettere all'Ufficio Privacy la copia degli atti con cui sono stati designati gli Amministratori di sistema.

Articolo 16 - Il Data Protection Officer

Ai sensi dell'art. 37 del GDPR, l'ASP designa il Responsabile della Protezione dei dati o Data Protection Officer (di seguito anche "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'incarico di DPO può essere conferito dal Titolare sia a un soggetto interno all'ASP sia esterno.

L'ASP pubblica i dati di contatto del DPO all'interno del sito aziendale, sezione "protezione dati

personali", e li comunica al Garante, in conformità alle indicazioni da questo impartite, nonché si assicura che il DPO sia tenuto a conoscenza delle questioni riguardanti la protezione dei dati personali.
Inoltre, l'ASP fornisce al DPO le risorse, umane, tecnologiche e strumentali necessarie per assolvere ai suoi compiti, accedere ai dati personali e ai trattamenti e mantenere la propria conoscenza specialistica.

Il DPO, sia interno che esterno, agisce in autonomia, potendo sempre interagire con i ruoli privacy di volta in volta coinvolti dalle questioni data protection sottoposte alla sua attenzione.

Al DPO sono attribuiti i seguenti compiti:

a. riferire direttamente al Direttore Generale dell'ASP sulle problematiche relative alla protezione dei dati personali;
b. informare e fornire consulenza al Direttore Generale dell'ASP, all'Ufficio Privacy e al Gruppo di Lavoro Privacy. Tramite l'ufficio privacy, il DPO fornisce consulenza e informa i Delegati e loro incaricati (quando nominati) e agli Autorizzati, in merito agli obblighi derivanti dalla normativa vigente in materia di protezione dei dati;
c. monitorare l'osservanza del presente Regolamento e delle altre disposizioni vigenti in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione dei Delegati e degli Autorizzati e alle connesse attività di controllo, scaturenti dalla raccolta di informazioni per individuare i trattamenti svolti, analisi e verifica di tali trattamenti in termini di loro conformità;
d. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
e. collaborare, solo se richiesto, con l'Ufficio Privacy nell'attività di predisposizione e aggiornamento della documentazione, delle linee guida, delle procedure, delle disposizioni operative e dei Registri del trattamento del Titolare e del Responsabile, nella formazione e negli audit, necessari a rendere operative le indicazioni di legge e del presente Regolamento;
f. portare a conoscenza l'ufficio privacy delle richieste ricevute da parte degli interessati e dei dipendenti/collaboratori ASP e delle eventuali azioni intraprese alimentando l'indispensabile flusso informativo per garantire un collegamento armonico in ambito data protection.
g. cooperare e fungere da punto di contatto con l'Autorità Garante per la Protezione dei Dati Personali per tutte le questioni connesse al trattamento dei dati personali, consultandolo quando necessario.

Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al trattamento dei dati, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. A tal fine, può proporre al Titolare l'ordine di priorità con il quale dar seguito alle problematiche poste alla sua attenzione, tenuto conto, mediante un approccio selettivo e programmatico, del maggiore rischio che queste possano comportare in termini di protezione dati, alla luce della documentazione e delle informazioni pervenute ed in particolare sulla base delle relative Valutazioni d'Impatto Privacy.
Il DPO, nei casi in cui ne è prevista la consulenza e/o il supporto, è tenuto a fornire il proprio riscontro nel termine di 5 (cinque) giorni dal ricevimento della richiesta pervenuta dal Titolare o altra Funzione privacy titolata. La mancata risposta è considerata quale silenzio-assenso del DPO rispetto alle attività presentate alla sua attenzione da parte del Titolare o altra Funzione privacy titolata.

La tempistica di cui sopra può subire delle variazioni quando:

- la normativa in materia di protezione dei dati prevede dei tempi più ristretti per la gestione degli adempimenti data protection ove il DPO è coinvolto dal Titolare (es. data breach);
- il presente Regolamento, le Procedure data protection o altre disposizioni regolatorie aziendali dispongano diversamente per specifiche attività ordinarie o straordinarie.

Articolo 17 – L'Ufficio Privacy

L'ASP ha istituito l'Ufficio Privacy, presieduto dal Responsabile del Servizio informativo aziendale, composto da personale qualificato sulle tematiche inerenti la data protection, facente funzioni all'interno del Servizio Informativo e della Transizione Digitale di ASP (di seguito anche "SITD") e che ha come contatto email a favore di tutto il personale dell'ASP, dei responsabili e degli interessati: *sitd.ufficioprivacy@asp.rg.it*

L'Ufficio Privacy si occupa dello svolgimento delle seguenti attività:

a. predisposizione di modulistica, standard, linee guida, procedure, registri e policy;
b. gestione centralizzata delle richieste interne in materia privacy;
c. indirizzo periodico degli adempimenti privacy, es. DPIA, lettere di nomina, informative, TVCC, impostazione attività by design & by default, etc.;
d. formazione;
e. audit di controllo interni;
f. attuazione delle misure tecniche e organizzative**.**
g. Monitoraggio e gestione, anche ai fini della data protection, del sistema di conservazione digitale

L'Ufficio Privacy, rappresentato da una persona incaricata e professionalmente qualificata, ricopre le seguenti funzioni:

- membro del Gruppo di Lavoro Privacy
- membro del coordinamento regionale dei DPO, in affiancamento al DPO aziendale

L'Ufficio Privacy, congiuntamente al Gruppo di Lavoro Privacy, si pone come interlocutore principale in materia privacy dell'ASP, con riferimento alla gestione dell'operatività e indirizzo delle principali questioni in ambito privacy. Il DPO fa riferimento all'ufficio privacy per qualunque questione inerente problematiche inerenti al trattamento dei dati.

L'ufficio Privacy potrà avvalersi, inoltre, dell'apporto di tutti gli ulteriori collaboratori aziendali che, in ragione della specifica professionalità, possano contribuire alla gestione delle attività ad esso riferite, quale misura essenziale dell'accountability e del Sistema Gestionale Privacy dell'ASP.

Articolo 18 – Il Gruppo di Lavoro Privacy

L'ASP ha, altresì, costituito il Gruppo di Lavoro Privacy, composto da membri che si contraddistinguono per esperienze, conoscenze e competenze diverse; nello specifico:

a. Ufficio Privacy rappresentato da persona incaricata e dal Responsabile del SITD che lo presiede;
b. Direttore Sanitario;
c. Direttori sanitari di presidi;
d. Direttori sanitari di distretto;
e. Direttori di dipartimento amministrativo.

I componenti del Gruppo di Lavoro Privacy, anche non in composizione plenaria, si riuniranno su convocazione dell'Ufficio Privacy, tutte le volte che le tematiche data protection lo richiederanno. Le consultazioni potranno riguardare tutte le questioni data protection gestite direttamente dall'Ufficio Privacy o ad esso riferite, con l'obiettivo di fornire un supporto maggiore a fronte di esigenze derivanti dal contesto che richiedono professionalità e competenze specialistiche.

A tal proposito, il Gruppo di Lavoro Privacy potrà avvalersi, inoltre, dell'apporto di tutti gli ulteriori collaboratori aziendali che, in ragione della specifica professionalità, possano contribuire alla gestione delle attività ad esso riferite, quale misura essenziale dell'accountability e del Sistema gestionale privacy dell'ASP.

Articolo 19 - I Facilitatori privacy

I direttori sanitari – amministrativi (facenti parte del gruppo di lavoro privacy) possono avvalersi di Facilitatori Privacy, previa designazione formale, per dirimere ulteriormente il rischio di approcci differenziati nella gestione degli adempimenti data protection nell'interesse di ASP. Le specifiche funzioni dei Facilitatori Privacy saranno stabilite nel relativo atto di designazione.

Articolo 20 - L' informativa all'Interessato

L'ASP adotta un sistema di documenti contenenti le informazioni sul trattamento dei dati personali degli interessati, formulate in modo tale da risultare chiare e comprensibili all'utenza, nonché funzionali a fornire all'interessato tutte le notizie sul trattamento dei propri dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

Le informazioni sul trattamento dei dati personali sono contenute nelle informative sul trattamento dei dati personali e riportano:

- l'identità e i dati di contatto del Titolare del trattamento;
- l'indicazione della nomina del DPO e i relativi dati di contatto;
- l'indicazione dell'Ufficio Privacy e i relativi dati di contatto;
- le finalità del trattamento dei dati personali nonché la relativa base giuridica;
- le modalità di trattamento dei dati personali;
- l'obbligatorietà o meno del conferimento dei dati;
- il periodo di conservazione dei dati personali oppure, in alternativa, i criteri seguiti per

determinare tale periodo;
- coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- i diritti riconosciuti agli interessati dalla normativa in materia di protezione dei dati personali e le modalità del relativo esercizio;
- qualora la liceità del trattamento dei dati sia basata sul consenso dell'interessato, l'informazione sulla possibilità di revocarlo in qualsiasi momento, senza pregiudizio sulla liceità del trattamento basato sul consenso svolto prima della revoca;
- il diritto di proporre reclamo all'Autorità Garante;
- se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure è un requisito necessario per la conclusione di un contratto;
- se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione e, in tali casi, le indicazioni significative sulla logica utilizzata, nonché sull'importanza e le conseguenze di tale trattamento per l'Interessato;
- nel caso in cui i dati personali non siano stati ottenuti presso l'Interessato, comunicazione della fonte da cui sono raccolti i suoi dati personali e, se applicabile, la specifica che i dati provengano da fonti accessibili al pubblico;
- l'eventuale trasferimento di dati personali al di fuori dell'Unione Europea e le misure adottate dal Titolare in conformità alla normativa vigente.

L'ASP, tramite l'Ufficio Privacy, coinvolgendo all'occorrenza il DPO, predispone informative specifiche, che descrivono ulteriori e particolari trattamenti di dati da questa svolti in determinati ambiti.

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 concordati dall'Ufficio Privacy, sentito, se reputato necessario, il Gruppo di Lavoro Privacy e il DPO.

L'ASP attiva, utilizzando diversi canali di comunicazione quali e-mail, home page, link dedicato, e sistemi Internet in genere, adeguate modalità di visibilità delle azioni poste in essere all'interno dell'ASP in attuazione della normativa sulla protezione dei dati.

Le informazioni sul trattamento dei dati personali possono non essere rilasciate all'Interessato da parte dell'ASP nel caso in cui questi disponga già delle suindicate informazioni o nel caso in cui comunicarle risulti impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, purché in tali casi siano state adottate preventivamente misure tecniche e organizzative adeguate per la protezione dei dati , specie al fine di garantire il rispetto del principio della minimizzazione dei dati, e ulteriori misure appropriate per tutelare i diritti e le libertà dell'interessato.
Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici; se richiesto dall'interessato, queste possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Articolo 21 - I diritti dell'Interessato

Gli Interessati possono contattare il Titolare, anche per il tramite dell'Ufficio Privacy, per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

I diritti esercitabili dall'Interessato sono prescritti agli artt. da 15 a 22 del GDPR, cui si aggiunge la possibilità di revoca del consenso, qualora previsto come base giuridica del trattamento.

L'Interessato ha il diritto di ottenere dall'ASP 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 seguiti 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 all'Autorità 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 di tale trattamento.

L'Interessato ha altresì il diritto di ottenere dall'ASP 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 può avanzare specifica istanza per l'esercizio dei propri diritti, preferibilmente nel rispetto delle modalità descritte nell'informativa e tramite i canali attivati dal Titolare.

L'Ufficio Privacy avvia le attività funzionali alla gestione della richiesta di esercizio dei diritti, avvalendosi, laddove necessario, anche dell'apporto e della collaborazione del DPO, del Delegato del trattamento dei dati di competenza e, all'occorrenza, degli Amministratori di Sistema interessati.

L'ASP disciplina con apposita procedura l'iter e le modalità del suindicato procedimento.

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 giuridicamente rilevante.

I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque abbia legittimo interesse, documentato nelle forme di Legge, anche mediante delega o procura a persone fisiche o ad associazioni, conferita per iscritto e nelle forme di Legge.

Articolo 22 - Diritto di opposizione

L'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e l'ASP si astiene dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono 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 riguarda, salvo che il trattamento sia necessario perl'esecuzione di un compito di interesse pubblico.

Articolo 23 - Il diritto di accesso e il diritto alla riservatezza

L'ASP, in osservanza delle disposizioni vigenti in tema di riservatezza e di trasparenza, valuta anche con riguardo ad altre regolamentazioni specifiche, caso per caso, la possibilità degli interessati di accedere ai propri dati personali.

L'accesso ai dati idonei a rivelare lo stato di salute o le abitudini sessuali è ammesso solo quando il diritto da tutelare, tramite istanza di accesso, è di rango almeno pari al diritto alla riservatezza, ovvero consiste in un diritto alla personalità o in un altro diritto o libertà fondamentale o inviolabile, quale ad esempio il diritto alla difesa.

Ulteriori specifiche indicazioni agli operatori sono contenute negli altri regolamenti o istruzioni operative adottate dall'ASP.

Articolo 24 - Comunicazione di dati all'Interessato

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo attraverso:

a. la consegna dei dati al medico di fiducia che, a sua volta, li renderà noti all'Interessato;
b. una spiegazione orale o un giudizio scritto da parte di un medico del servizio interessato o, su specifica delega scritta, da parte di operatore sanitario;
c. modalità telematiche nei casi e nei modi previsti dalla specifica normativa.

La documentazione sanitaria che viene consegnata in busta chiusa può essere ritirata dall'Interessato o da altra persona diversa da questo, se delegata, salvo il caso dei documenti relativi a dati regolati da normative speciali che prevedono il ritiro diretto dell'interessato.

Articolo 25 - La comunicazione dei dati personali all'esterno (destinatari)

La comunicazione dei dati personali all'esterno dell'ASP, previa opportuna informazione resa all'Interessato, è effettuata esclusivamente nei seguenti casi:

- ad enti o aziende del SSN, della Pubblica Amministrazione e ad altri soggetti di natura pubblica e privata, in esecuzione di obblighi derivanti da normative vigenti o per lo svolgimento delle funzioni istituzionali;
- qualora la comunicazione di dati personali ad altro soggetto pubblico che sia prevista da provvedimenti dell'Autorità diversi dalla normativa, ovvero previa comunicazione alla stessa Autorità Garante.

La suindicata trasmissione dei dati personali avviene in forma scritta o telematica, ovvero in qualsiasi altra modalità che si dovesse rendere necessaria in base alle circostanze del caso.

Articolo 26 - Le informazioni sullo stato di salute dell'interessato

I dati personali inerenti alla salute possono essere comunicati all'Interessato o a soggetto da questi autorizzato, solo dal personale medico, salvo specifica autorizzazione scritta dell'ASP ad un diverso operatore del ruolo sanitario, in casi motivati e salvo il caso in cui i dati personali siano stati forniti in precedenza dal medesimo Interessato.

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

A tal fine, l'ASP 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 ne esercita la responsabilità genitoriale o la tutela legale.

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.

Articolo 27 - La trasmissione e l'interscambio dei dati personali tra le strutture dell'ASP

L'ASP assicura che la comunicazione o l'interscambio di dati personali in ambito aziendale per l'espletamento delle finalità istituzionali è effettuata soltanto nei limiti del principio di necessità e minimizzazione in relazione allo scopo del trattamento, osservando le disposizioni del presente Regolamento e le relative misure di sicurezza.

Articolo 28 - La diffusione dei dati personali e particolari

La diffusione dei dati personali, comuni, particolari e/o relativi a condanne penali o reati, in ambito aziendale è consentita soltanto per adempiere ad obblighi previsti dalle normative vigenti e nelle forme da queste previste, in particolare l'obbligo di trasparenza al quale è soggetta l'amministrazione.
La diffusione a terzi di qualsiasi dato di natura particolare e/o relativo a condanne penali o reati è comunque assolutamente vietata.

Articolo 29 - La politica di sicurezza aziendale

L'ASP, 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 tecniche e organizzative.

A riguardo l'ASP 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:

a. «liceità, correttezza e trasparenza», cioè siano trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b. «limitazione della finalità», cioè siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
c. «minimizzazione dei dati», cioè questi debbano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d. «esattezza», cioè siano 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;
e. «limitazione della conservazione», cioè siano 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 richieste dal presente regolamento a tutela dei diritti e delle libertà dell'Interessato;
f. «integrità e riservatezza», cioè 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;
g. «responsabilizzazione», cioè adottando e essendo in grado di dimostrare che il trattamento dei dati viene svolto nel pieno rispetto della normativa vigente.
h.

Articolo 30 - La protezione dei dati personali fin dalla progettazione (c.d. privacy by design) e la protezione dei dati per impostazione predefinita (c.d. privacy by default).

Per l'ASP il Sistema gestionale privacy è un requisito indispensabile di qualità per assicurare la protezione dei dati personali sin dalla progettazione; tale sistema prevede l'adozione di tutte le misure tecniche e organizzative necessarie a far sì che la protezione dei dati personali e la loro tenuta in sicurezza consentano non solo il rispetto di un obbligo normativo, ma anche una crescita organizzativa e culturale capace di innovare l'ASP stessa e di coinvolgere efficacemente tutti i suoi collaboratori.

L'ASP al momento di determinare le modalità e gli strumenti del trattamento, tenendo conto dello stato dell'arte, costi di attuazione, natura, ambito di applicazione, contesto e finalità del trattamento e dei possibili rischi aventi probabilità e gravità diverse che questo potrebbe comportare per i diritti e le libertà degli Interessati, mette in atto misure tecniche e organizzative adeguate a integrare nel trattamento stessole garanzie necessarie a soddisfare i requisiti normativi e tutelare i diritti degli Interessati.

L'ASP, altresì, mette in atto misure tecniche e organizzative adeguate, già in fase progettuale, per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, sia per quanto riguarda, in particolare:

- la quantità dei dati personali raccolti;
- la portata del trattamento;
- il periodo di conservazione;
- l'accessibilità.

Tali misure garantiscono inoltre che, per impostazione predefinita, i dati personali siano accessibili solo alle persone autorizzate e limitatamente a quanto necessario per il periodo di trattamento.

Articolo 31 - La Valutazione di Impatto sulla protezione dei dati e la consultazione preventiva con l'Autorità Garante della protezione dei dati

L'ASP, prima di iniziare un trattamento dei dati personali, per il tramite dell'Ufficio Privacy si assicura che venga effettuata un'apposita valutazione preliminare dell'impatto delle operazioni di trattamento sui diritti e le libertà degli Interessati coinvolti, avvalendosi e consultandosi, qualora necessario, con il proprio DPO.

La Valutazione di Impatto preliminare viene effettuata dall'ufficio privacy nei casi e nei modi previsti dalle disposizioni vigenti, al fine di valutare:

- i rischi del trattamento;
- le misure previste per contenerli;
- le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare laconformità alle norme vigenti, tenuto conto dei diritti degli interessati e delle finalità del trattamento.

L'ASP disciplina con apposita procedura l'iter e le modalità della Valutazione di Impatto Privacy.

La documentazione relativa ad ogni valutazione preliminare di impatto viene conservata all'interno del Sistema gestionale privacy aziendale ed eventualmente trasmessa al DPO.

Tale valutazione, se necessario, è sottoposta a riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato l'ASP, prima di procedere al trattamento, consulta l'Autorità Garante.

L'ASP, inoltre, attiva tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche individuate dall'Autorità Garante per il corretto trattamento dei dati, in modo particolare per quanto riguarda i trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi sanitari integrati.

Articolo 32 - Le misure di sicurezza

L'ASP, anche attraverso le diverse figure previste dal Modello organizzativo privacy di cui si è dotata (ad es. Delegati, incaricati alla gestione, Autorizzati, etc.) è tenuta ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura di sicurezza necessaria ad assicurare un livello adeguato di sicurezza dei dati personali trattati.

Questa, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
Tali misure comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente disponibilità e accesso dei dati personali in caso di incidente;
- una procedura per testare, 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 tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Tutti coloro che trattano dati per conto dell'ASP possono trattare dati personali solo se autorizzati e istruiti in tal senso dall'ASP stessa.

L'accesso ad ogni risorsa informatica è consentito solo se congruente con il trattamento di dati per il quale il collaboratore dell'ASP è stato precedentemente designato Autorizzato ed è consentito soltanto utilizzando apposite credenziali di autorizzazione composte da un user-id e da una password, attribuite dall'Amministratore di Sistema di competenza.
La richiesta di rilascio delle credenziali per accedere alla risorsa informatica, una volta sottoscritta dal Delegato, è inoltrata all'Amministratore di Sistema di competenza che, una volta attribuitele relative credenziali, le custodisce presso il Servizio Informativo aziendale.

L'Ufficio Privacy, con l'eventuale supporto del DPO solo se richiesto, verifica periodicamente, in sede di audit, la congruenza della nomina ad Autorizzato con la richiesta di rilascio delle credenziali.

La password è strettamente personale e a nessun titolo può essere comunicata a terzi. Della sua riservatezza risponde personalmente il singolo Autorizzato.

Il Delegato è tenuto a comunicare agli Amministratori di Sistema e all'Ufficio Privacy la data di cessazione dell'incarico al trattamento dei dati da parte del suo collaboratore.

Spetta alla Direzione risorse umane comunicare all'Ufficio Privacy e all'Amministratore di Sistema gli aggiornamenti e le variazioni relative al personale (cessazioni, sostituzioni, incarichi, aspettative, assenze prolungate per almeno 180 gg, trasferimenti, ecc.) che comportano una modifica al sistema delle autorizzazioni al trattamento dei dati personali.

L'ASP adotta, entro il 30 giugno di ogni anno, un Documento Analisi e Valutazione Rischi (di seguito DAVR), che:
- individua le misure adeguate a elevare lo standard di sicurezza dei dati anche sulla base dell'analisi dei rischi;
- rappresenta la distribuzione dei compiti e delle responsabilità del trattamento dei dati;
- programma l'attività di formazione dei Delegati, degli Autorizzati e Amministratori di Sistema al fine di un utilizzo consapevole delle informazioni;
- evidenzia le misure che l'ASP ha adottato nel tempo per proteggere i dati personali a sua disposizione eil piano delle azioni di miglioramento che intende adottare per l'anno in corso.

Il DAVR è predisposto dall'Ufficio Privacy, con l'eventuale coinvolgimento del DPO, con il supporto del SITD al quale resta in carico fornire e produrre tutte le informazioni e documentazioni afferenti specificamente il predetto Servizio Informatico, tali da consentire all'Ufficio Privacy, la produzione del documento in oggetto corredato dalle specifiche misure tecniche e organizzative adeguate.

Su richiesta dell'Ufficio Privacy, i Delegati devono inviare, una relazione annuale sul loro operato, che deve evidenziare:
- l'attività svolta e le misure di sicurezza adottate;
- le carenze strutturali e organizzative;
- le specifiche necessità formative necessarie per l'attuazione delle disposizioni sulla riservatezza;
- le criticità di sicurezza riscontrate;

- le contromisure di cui si propone l'attivazione.

Articolo 33 - Le misure di sicurezza per i trattamenti di dati personali affidati a soggetti esterni

I Responsabili e Sub-Responsabili sono tenuti ad assicurare al Titolare del trattamento di aver adottato, prima di effettuare attività di trattamento di dati, misure tecniche e organizzative adeguate secondo quanto previsto dalla normativa vigente in tema di protezione di dati e amministrazione digitale.

Tali soggetti sono comunque tenuti ad assicurare il rispetto delle specifiche istruzioni operative impartite dall'ASP per la tenuta in sicurezza dei dati oggetto di affidamento e di aver ulteriormente attivato ogni altramisura idonea alla protezione dei dati loro affidati.

Su richiesta dell'Ufficio Privacy, i Responsabili sono tenuti ad inviare all'Ufficio Privacy una relazione dettagliata nella quale sono evidenziate:

- l'attività svolta e le misure di sicurezza adottate;
- l'elenco degli autorizzati del trattamento e l'indicazione della sede presso la quale i relativi atti di nomina sono custoditi;
- l'elenco delle risorse hardware e software disponibili e utilizzate;
- le procedure di continuità operativa ed emergenza adottate;
- le misure di recupero da disastro adottate;
- le misure di back-up del sistema informativo aziendale e di contenimento dei virus informatici adottate,comprese quelle di conservazione sostitutiva;
- le eventuali criticità che potrebbero costituire occasione di accesso non consentito o perdita/manomissione del patrimonio informativo gestito 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, rimettendo alriguardo anche la relativa documentazione;
- le verifiche periodiche sul mantenimento in sicurezza che sono state adottate, con la relativa documentazione.

Nel caso in cui il Responsabile, nell'esecuzione delle attività di trattamento, utilizzi strumenti informatici propri, è tenuto a attestare con una propria dichiarazione scritta di assicurare la protezione dei dati affidati dal Titolare attraverso specifiche misure adeguate di sicurezza e non aver affidatoalcune fasi del trattamento a soggetti terzi, salvo che l'ASP non abbia autorizzato la nomina di questi come Sub-responsabile.

A tale proposito, è fatto obbligo all'Ufficio Privacy di acquisire da parte del Responsabile specifica attestazione circa la corretta adozione di misure tecniche ed organizzative adeguate, regolarmente e periodicamente aggiornate.

Qualora il Responsabile utilizzi, al contrario, strumenti informatici forniti dall'ASP, è tenuto a trasmettere copia degli atti di designazione ad Autorizzati all'Ufficio Privacy, che provvederà ad attivare

le procedure necessarie al rilascio delle relative credenziali di accesso.

Il mancato rispetto da parte del Responsabile delle misure di tecniche e organizzative adeguate a contenere o prevenire rischi che possono riguardare i dati oggetto dell'affidamento può costituire titolo per larescissione del rapporto sottostante e per chiedere un eventuale risarcimento del danno.

Articolo 34 - Gli interventi tecnici a cura di soggetti esterni

I soggetti esterni che, in forza di un rapporto contrattuale con l'ASP, esercitino attività di manutenzione su apparecchiature utilizzate per il trattamento o la registrazione di dati, 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'ASP 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'ASP.

Articolo 35 - La tenuta in sicurezza dei documenti e archivi di titolarità dell'ASP

Gli archivi che custodiscono i dati di cui è titolare del trattamento l'ASP, 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.

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 Delegato dispone, attenendosi alle indicazioni del Titolare e alle disposizioni e Procedure Aziendali vigenti, i criteri necessari a garantire un accesso controllato ai locali e un accesso selezionato ai dati, mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario diservizio degli Archivi medesimi.

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 nei modi e termini previsti dalla normativa vigente.

L'accesso agli archivi cartacei aziendali è formalmente autorizzato, da parte dei Delegati.

Relativamente agli archivi digitali il rilascio di tale autorizzazione è di competenza dell'Amministratore di Sistema, previa indicazione del Delegato e comunicazione all'Ufficio Privacy.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Delegato 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'ASP predispone un piano di scarto d'archivio, approvato con apposita deliberazione.

Relativamente agli archivi informatizzati di dati e di esclusiva pertinenza del SITD, l'ASP adotta, facendo seguito alle disposizioni vigenti secondo standard e norme in tema di protezione dati e amministrazione digitale, in stretta collaborazione con l'Ufficio Privacy che monitorizza anche il sistema di conservazione digitale, i Delegati, i Responsabili (se necessario) e gli Amministratori di Sistema, idonee procedure di:

- salvataggio periodico degli archivi di dati personali;
- misure di contenimento dei virus informatici;
- disaster recovery;
- continuità operativa;
- conservazione digitale.
- conservazione sostitutiva

Resta obbligatorio da parte di qualunque dei suddetti soggetti segnalare eventuali criticità e problematiche al Titolare ed all'Ufficio Privacy, che si occuperanno dell'eventuale allineamento al DPO.

Articolo 36 - I limiti alla conservazione dei dati personali

L'ASP, anche per il tramite dell'ufficio privacy, assicura l'adozione di apposite misure e procedure attraverso le quali si determinano:

- le modalità con cui procedere alla distruzione dei documenti analogici e digitali, una volta terminato il limite massimo diconservazione dei documenti e dei dati in questi riportati;
- i criteri di smaltimento degli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l'ASP;
- i parametri di riutilizzo di apparati di memoria o hardware, affinché sia effettuato con modalità tali da assicurare che non sia possibile accedere ad alcun dato personale di cui è titolare l'ASP.

Articolo 37 - Le attività di verifica e controllo dei trattamenti di dati personali

L'ASP 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

trattamentodei dati da parte dei Delegati, Responsabili, 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 dall'Ufficio Privacy, con la collaborazione del DPO laddove ritenuto necessario.

Articolo 38 - La formazione di Delegati, Autorizzati e Amministratori di sistema

L'ASP, inserisce nel proprio Piano Annuale di Formazione iniziative atte ad assicurare la formazione il continuo aggiornamento dei Delegati, degli Autorizzati da questi coordinati, degli Amministratori di Sistema, degli ulteriori ruoli privacy eventualmente nominati dal Titolare 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 a cura dell'Ufficio Privacy.

I Responsabili e i Sub-Responsabili sono tenuti a assicurare all'ASP 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.

Articolo 39 - La violazione dei dati personali
(concetti base con riferimento alla procedura aziendale deldata-breach)

Ogni Responsabile, Delegato o Autorizzato è tenuto a informare senza ingiustificato ritardo l'Ufficio Privacy, che allineerà prontamente il DPO, del possibile caso in cui si sia verificata una violazione dei dati personali (cfr "Procedura per la gestione dei Data Breach, adottata con deliberazione n. 1466/2018).

Anche ogni Interessato, utilizzando l'apposito indirizzo mail può segnalare al Titolare (direzione.generale@asp.rg.it) e/o al Data Protection Officer (dpo@asp.rg.it), nonché all'Ufficio Privacy (sitd.ufficioprivacy@asp.rg.it), un possibile caso di violazione dei dati personali.

In tali casi, l'ASP avvia le necessarie procedure e, avvalendosi anche della collaborazione dei Delegati, accerta lo stato dell'arte.

L'ASP provvede a notificare attraverso il Data Protection Officer la violazione all'Autorità Garante 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 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 libertàdegli Interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente.

La notifica 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 della 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 attenuarne 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.

Articolo 40 - La disciplina delle misure del Regolamento

Nelle forme e con le modalità previste dal sistema di qualità aziendale l'ASP provvede ad adottare procedure, disciplinari, Linee Guida e Indicazioni Operative e Regolamenti di settore che consentano l'applicazione del presente Regolamento e delle previsioni di legge volte ad assicurare la protezione dei dati personali.

L'ASP 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.

Articolo 41 - Le norme transitorie e finali

Per tutto quanto non espressamente previsto dal presente Regolamento si applica la normativa vigente in tema di protezione dei dati personali e amministrazione digitale.
L'ASP si riserva, inoltre, di adeguare, modificare o integrare il testo del presente Regolamento a fronte di sopravvenute esigenze organizzative ovvero mutamenti della disciplina normativa applicabile.