Regione Siciliana
AZIENDA SANITARIA PROVINCIALE SIRACUSA
Cod.Fisc. e P.IVA: 01661590891

Direzione Generale
Corso Gelone n. 17 - 96100 Siracusa

REGOLAMENTO AZIENDALE
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

sulla base del
Regolamento Europeo 679/2016 del Parlamento Europeo e del Consiglio del 27 Aprile 2016

Sommario

Premessa

Il presente Regolamento è stato predisposto per regolare, attraverso una serie di misure che compongono un vero e proprio "sistema gestionale privacy", i compiti e le responsabilità di tutti coloro che nell'ASP trattano dati personali.

Il documento, che è stato elaborato tenendo conto dell'attuale quadro regolatorio, 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 (regolamento generale sulla protezione dei dati), sia dalle indicazioni del Decreto Legislativo n.196 del 2003 così come adeguato dal D.Lgs. n . 101/2018 e succ. m m. e ii., 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 2003 "Codice in materia di protezione dei dati personali" così come adeguato dal decreto legislativo n.101 del 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 (regolamento generale sulla protezione dei dati)
Decreto Legislativo n. 82 del 2005 "Codice dell'Amministrazione digitale" e succ . mm. e ii.;
Legge 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e ss. m m.ii;
e, Decreto Legislativo n. 33 del 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 succ. mm. e ii.;
e Linee guida in tema di Fascicolo sanitario elettronico (FSE) e Dossier sanitario del 16 luglio 2009;
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;
Linee guida in materia di Dossier sanitario del 4 giugno 2015 .

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 servIzI0 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) «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;
j) «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;
k) «Interessato»: persona fisica cui si riferiscono i dati personali;
l) «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;
m) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso , mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
n) «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;
o) «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 fi sica , e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
p) «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;
q) «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;
r) «Dati identificativi»: i dati personali che permettono l'identificazione diretta dell'interessato;
s) «Dati giudiziari» i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
t) «Dati sensibili»: 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;
u) «Dato anonimo»: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

v) «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;
w) «Autorità Garante Privacy»: 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 documento individua le politiche aziendali relative alla corretta gestione del trattamento dei dati personali, così come definiti dal "Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (di seguito GDPR), dal Decreto Legislativo n. 196 del 2003 "Codice in materia di protezione dei dati personali" così come modificato dal Decreto Legislativo n.101 del 2018 e dai Provvedimenti del Garante per la Protezione dei Dati, attraverso l'individuazione di una serie di misure che compongono un vero e proprio "Sistema Gestionale Privacy", nonché di compiti e di 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 con 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 devono trattarli, adotta misure capaci di assicurare e documentare che il trattamento dei dati personali viene effettuato con modalità tali da preservarne l'integrità e la confidenzialità, nel rispetto delle adeguate misure di sicurezza.
A riguardo, I' 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 confronti dell'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 per 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 di 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, adottando politiche adeguate in materia di protezione dei dati.

Tali misure compongono il sistema gestionale privacy aziendale, che include:

- Il Gruppo di lavoro Privacy";
- 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;
- 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, Autorizzati del trattamento ed Amministratori di sistema;
- il sistema di relazione con gli Interessati.
- L'ASP integra il Sistema gestionale privacy al fine di realizzare un sistema integrato 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.

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.

I dati personali trattati comprendono anche le seguenti tipologie di dati sensibili:

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

Nei casi e con i limiti previsti dalle normative di settore vigenti, I' ASP, altresì, tratta dati personali e sensibili per la rilevazione delle malattie mentali, malattie infettive e diffusive e 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 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, o presso altri esercenti professioni sanitarie .

Per effettuare il trattamento dei dati personali, I' 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 previsti dalla normativa vigente. soltanto previa erogazione di apposita informativa ed adozione di apposite ed adeguate misure di sicurezza .

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

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 - L'autorizzazione al trattamento dei dati personali

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

Il trattamento dei dati suindicati è effettuato, qualora la legge o i Provvedimenti dell'Autorità Garante per la protezione di dati personali lo prevedano, previa acquisizione della specifica autorizzazione da parte degli Interessati.

Il Titolare assicura, attraverso idonee modalità, l'archiviazione di tali autorizzazioni in modo da renderle fruibili e rintracciabili.

Articolo 7 - Il trattamento dei dati personali

Il trattamento dei dati personali è ammesso solo da parte del Titolare del trattamento dei dati, dei Delegati, degli Autorizzati/Incaricati e degli Amministratori di Sistema, dei Responsabili del trattamento e degli eventuali Sub-Responsabili del trattamento.

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.

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

I 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.

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

I Delegati sono tenuti a comunicare dati personali e/o sensibili 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 pre-configurati, in ossequio al già citato 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 dell'Autorità Garante

Articolo 8 - Il trattamento dei dati sensibili o categorie di dati particolari di dati

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 fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
e) il trattamento è necessario per motivi di interesse pubblico rilevante che deve essere proporzionato alla finalità perseguita;
f) il trattamento è necessario per rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
g) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali o conformemente al contratto con un professionista della sanità;

h) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
i) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Qualora il trattamento sia basato sul consenso, è compito dell'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 materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

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

Articolo 9 - Il controllo a distanza

Ad ogni sistema di controllo a distanza, degli Interessati e/o del lavoratore, I' 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 compreso il rispetto 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 delle attività di trattamento svolte sotto la propria responsabilità, costantemente aggiornato a cura del Data Protection Officer, 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
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 forma scritta, anche in formato elettronico e, su richiesta, viene messo a disposizione dell'Autorità Garante Privacy.

Articolo 11- Il Titolare del trattamento dei dati personali

Il Titolare del trattamento dei dati personali è I'ASP, 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, che il trattamento dei dati personali di riferimento aziendale è effettuato conformemente alla normativa vigente.

Nel caso in cui I'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

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

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

Il Titolare, tramite il Data Protection Officer di cui agli articoli 31 e 32 del presente regolamento, provvede, nei casi previsti dalla legge:

a) ad assolvere ogni obbligo di comunicazione, interpello o notificazione, all'Autorità Garante per la Privacy;
b) a cooperare, su richiesta, con l'Autorità Garante per la Privacy nell'esecuzione dei suoi compiti;
c) a richiedere a tale Autorità ogni necessaria autorizzazione al trattamento dei dati personali, ove necessaria;
d) ad adottare, per quanto di competenza, le misure necessarie a garantire la protezione dei dati personali, anche per quanto riguarda il processo di digitalizzazione;
e) a designare il Data Protection Officer, dotandolo delle necessarie ed 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 effettuati in ASP di cui al successivo art. 15;
h) ad assicurare l'informazione e la formazione del personale sul tema della tutela della riservatezza dei dati personali;
i) a nominare i Delegati, Responsabili del trattamento e Sub-Responsabili del trattamento di dati personali impartendo loro le necessarie istruzioni per la corretta gestione e protezione dei dati personali.

Il Titolare del trattamento è tenuto, in base alle disposizioni vigenti in materia di protezione dei dati, ad effettuare nei confronti di tutti i Responsabili del trattamento le verifiche e controlli sulla correttezza del trattamento dei dati personali loro delegato.

Articolo 12- I Responsabili del trattamento dei dati personali e i (sub-responsabili)

L'ASP designa Responsabili del trattamento dei dati personali tutti i soggetti esterni cui sono delegate attività di competenza aziendale o attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comunque comportano necessariamente il trattamento dei dati personali.

L'ASP designa quali Responsabili del trattamento dei dati personali esclusivamente i soggetti che presentino 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 dell'interessato.

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

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

Tale contratto, stipulato in forma scritta, anche in formato elettronico, prevede, in particolare, che il Responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata dell'ASP;
b) garantisca che gli Autorizzati del trattamento dei dati personali siano sottoposti a mantenere la riservatezza di tali dati;
c) adotti tutte le misure di sicurezza indicate dall'ASP e le ulteriori misure tecniche e organizzative capaci di garantire ai dati oggetto di trattamento 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) tenendo conto della natura del trattamento, assista I' ASP con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfarne l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato 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 gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento 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, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso in cui un Responsabile del trattamento ricorra, previa specifica autorizzazione, a un Sub- Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'ASP, a tale altro Sub-Responsabile del trattamento sono imposti, mediante un contratto, gli stessi obblighi a cui è stato sottoposto il Responsabile. Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti delI' ASP l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile.

In tutti gli atti che disciplinano rapporti con i soggetti di cui al precedente comma (contratti, convenzioni, scritture private, conferimenti, etc.), deve inoltre essere inserita l'indicazione che I' ASP provvederà a designare successivamente, ma prima di procedere al trattamento dei dati, il contraente quale Responsabile del trattamento dei dati personali e a impartire le specifiche disposizioni operative.

Tutte le strutture interne all'ASP che provvedono alla stesura o validazione degli atti con cui sono delegate attività di competenza aziendale o attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comunque comportano necessariamente il trattamento dei dati personali, sono tenute a segnalare l'affidamento in itinere al Data Protection Officer, che provvederà a predisporre l'apposita documentazione.

Articolo 13 - I Delegati del trattamento dei dati personali e relativi compiti

L'ASP designa i Delegati del trattamento dei dati personali cui delegare il coordinamento delle attività di trattamento dei dati. I Delegati sono designati dal Titolare con apposito atto formale ed è accompagnato da specifiche indicazioni operative per il corretto assolvimento dei compiti a questi delegati in materia di protezione dei dati e dovrà essere notificata per iscritto ai Delegati a cura del Data Protection Officer.

L'ASP designa i Delegati del trattamento dei dati personali tra coloro che ricoprono gli incarichi di:

- Direttore Amministrativo pro-tempore, per i trattamenti afferenti agli uffici di Segreteria Generale ed 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 afferenti l' 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 e funzionale nonché i Responsabili delle unità operative complesse , dipartimentali e semplici afferenti detto dipartimento;
- Direttore di Distretto Sanitario
- Direttore di Presidio Ospedaliero

Sono designati altresì quali Delegati del trattamento:

- i dipendenti che svolgono attività libero-professionale intra-moenia;
- i Responsabili degli studi clinici ed osservazionali limitatamente ai trattamenti che da tale attività derivano.

La nomina è effettuata con atto predisposto dal Data Protection Officer ed indica i trattamenti di dati dei quali viene conferita la responsabilità del coordinamento.

L'ASP designa quali Delegati del trattamento dei dati esclusivamente i soggetti che presentino 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 dell'interessato.

L'Azienda , tramite il Data Protection Officer, conserva nel proprio sistema documentale privacy l'originale degli atti di designazione a Delegati del trattamento dei dati personali.

I Delegati del trattamento dei dati personali si attengono agli obblighi individuati dalla normativa vigente e dal presente Regolamento e, più specificamente, ai compiti e alle istruzioni notificati anche unitamente alla comunicazione della nomina a cura del Data Protection Officer.

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 al Data Protection Officer ogni conferimento o modifica di responsabilità in ambito aziendale affinché questi possa predisporre gli atti necessari alla designazione dei Delegati del trattamento dei dati personali.

La funzione di Delegato del trattamento dei dati personali è attribuita personalmente e non è suscettibile di delega.

L'elenco dei Delegati del trattamento dei dati in ambito aziendale è tenuto a cura del Data Protection Officer.

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 il Data Protection Officer 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 rpd@asp.sr.it.

Delegati del trattamento dei dati personali 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 fare osservare:

- 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, le ulteriori linee guida sulla riservatezza dei dati, la protezione delle informazioni e sull'amministrazione digitale.

I Delegati del trattamento dei dati sono dotati di autonomia gestionale ed 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.

E' compito dei Delegati del trattamento dei dati verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza rispondano ai principi di necessità, pertinenza e non eccedenza, segnalando al Data Protection Officer eventuali situazioni di potenziale compromissione della protezione dei dati personali.

I Delegati del trattamento, relativamente al proprio settore di competenza, rispondono al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale e riferiscono periodicamente al Data Protection Officer su come svolgono i compiti specifici loro assegnati e segnalano appena possibile ogni problematica di riferimento.

I Delegati del trattamento designano formalmente gli Autorizzati del trattamento, fornendo loro per iscritto istruzioni operative dettagliate e specifiche sulle corrette modalità di trattamento dei dati personali e vigilano sul rispetto di tali istruzioni, anche attraverso verifiche periodiche.

Articolo 14 - Gli autorizzati del trattamento dei dati personali: incaricati, tirocinanti e/o equiparati

Gli Incaricati del trattamento dei dati personali sono le persone fisiche che effettuano le operazioni di trattamento di dati personali e/o sensibili, autorizzati e designati a tale scopo dal Delegato o dal Responsabile del trattamento dei dati personali.
Sono da designare come Incaricati sia i dipendenti dell'ASP che i collaboratori che, a qualsiasi titolo (ad esempio: tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti), prestino la loro opera, anche in via temporanea , all'interno delle strutture dell'Azienda.

Per la loro designazione è utilizzata apposita modulistica, che prevede la trascrizione della data di inizio e eventuale fine dell'attività all'interno della struttura ed indica i trattamenti di dati di cui sono autorizzati a svolgere le relative operazioni.

Gli Incaricati ricevono formale atto di designazione dai loro Delegati del trattamento, che impartiscono loro disposizioni sul corretto uso dei dati, in special modo sotto il profilo della sicurezza e vengono informati sulle direttive vigenti sulla protezione dei dati da loro trattati.

L'atto di designazione ad Incaricato costituisce l'unico presupposto di liceità per il trattamento dei dati personali; l'originale di tale atto, controfirmato per presa visione dallo stesso incaricato, è trasmesso al Data Protection Officer, che ne cura la conservazione e ne inserisce i dati all'interno del Registro delle attività di trattamento.

Una copia dell'atto di nomina a Incaricato viene consegnata al designato e un'altra copia viene conservata dal Delegato del trattamento dei dati, che comunica al Data Protection Officer via mail e senza ritardo la data di cessazione dell'incarico.

La designazione ad Incaricato del trattamento dei dati personali 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 Incaricati del trattamento dei dati personali:

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.

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

In tale ultima ipotesi, tali Responsabili del trattamento conservano presso la loro sede legale gli originali degli atti di designazione ad Incaricato del trattamento e ne inviano copia via mail al Data Protection Officer.

Articolo 15 - Gli Amministratori di sistema

L' ASP designa i propri Amministratori di sistema con apposito atto, il cui originale viene conservato presso il Data Protection Officer, corredato di specifiche istruzioni operative e impartisce le opportune disposizioni perché sia assicurata l'effettività di tutte le misure ed audit previste dalla normativa vigente in tema di Amministratore di Sistema.

Gli Amministratori di sistema sono tenuti al rilascio agli Incar icat i del trattamento delle credenziali per accedere alle procedure informatiche previa richiesta sottoscritta dal Delegato del trattamento di riferimento.

GlI stessi sono inoltre tenuti a inoltrare le richieste suindicate al Data Protection Officer che li conserva assieme agli originali degli atti di nomina ad Incaricato e ne verifica la congruità.

Per quanto riguarda i soggetti esterni designati Responsabili e Sub-Responsabili del trattamento dei dati cui sono 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, compreso il rispetto delle misure di controllo dell'attività. Tali Responsabili e Sub-Responsabili sono pertanto tenuti ad assolvere a tutte le misure ed audit previste dalla normativa vigente in tema di Amministratore di Sistema ed a trasmettere al Titolare del trattamento sia l'evidenza delle nomine e delle ulteriori misure adottate sia la copia della relativa documentazione entro il mese di gennaio di ogni anno solare.

Tali Responsabili e Sub-Responsabili del trattamento sono tenuti a depositare presso il Data Protection Officer la copia degli atti con cui sono stati designati gli Amministratori di sistema.

Articolo 16 - Il Data Protection Officer (DPO) dell'ASP

L'ASP, giusta deliberazione n.464/2018, ha designato, al proprio interno, il Responsabile della Protezione dei dati o Data Protection Officer, individuando 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'ASP ne pubblica i dati di contatto e li comunica all'Autorità Garante Privacy, in conformità alle indicazioni da questa impartite e si assicura che il Data Protection Officer sia tempestivamente e adeguatamente coinvolto su tutte le questioni riguardanti la protezione dei dati personali e gli fornisce 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 Data Protection Officer agisce in totale autonomia operativa e opera in stretta collaborazione con il suo Staff, assieme al quale attiva tutte le misure per favorire l'osservanza del presente regolamento e delle altre disposizioni vigenti relative alla protezione dei dati ed ha i seguenti compiti:
riferire direttamente al Direttore Generale dell'ASP sulle problematiche relative alla protezione dei dati personali;
informare e fornire consulenza al Direttore Generale del!'ASP, ai Delegati del trattamento ed Autorizzati del trattamento dei dati personali, di cui al superiore articolo 13, in merito agli obblighi derivanti dalla normativa vigente in materia di protezione dei dati;
sorvegliare l'osservanza del presente regolamento e delle altre disposizioni vigenti relative alla protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione dei Delegati e degli Autorizzati del trattamento 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;
fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare lo svolgimento;
predisporre, anche su iniziativa del Titolare, la modulistica, le linee guida, procedure, disposizioni operative, registri e policy necessaria rendere operative le indicazioni di legge e del presente regolamento;
cooperare e fungere da punto di contatto per l'Autorità Garante Privacy per tutte le questioni connesse al trattamento dei dati personali, consultando quando necessario.

Nell'eseguire i propri compiti, il Data Protection Officer 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 , propone 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 .

Articolo 17- Il Gruppo di lavoro privacy

L'ASP, giusta delibera n. 1026/2018, in coerenza al Regolamento (UE) del Parlamento Europeo n.679/ 2016, ha istituito l'Ufficio del Data Protection Officer, quale supporto strutturale - organizzativo, in staff al vertice gerarchico del Titolare del trattamento.

A supporto specifico dell'Ufficio del Data Protection Officer, I'ASP ha altresì costituito il Gruppo di lavoro Privacy, coordinato dallo stesso Data Protection Officer, contraddistinto per esperienze, conoscenze e competenze diverse, così composto:

- Responsabile Affari Legali
- Responsabile Servizi Informativi;
- Responsabile Pianificazione;
- Referente Processi Sanitari;
- Referente Processi Amministrativi

Al fine di individuare e mettere in atto le misure tecniche ed organizzative adeguate per 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 di t ratt am ent o, il Data Protection Officer potrà avvalersi, inoltre, dell'apporto di tutti gli ulteriori collaboratori aziendali che, in ragione della specifica professionalità, possano contribuire alla gestione delle attività del gruppo, che costituisce misura essenziale dell' accountability e del Sistema gestionale privacy dell' ASP.

Articolo 18 - I Facilitatori privacy

L'ASL si avvale di una rete di collaboratori, denominati Facilitatori Privacy di struttura, che, all'interno di ogni struttura aziendale, supportano le azioni tese al rispetto delle normative sulla riservatezza, trasparenza e amministrazione digitale.

Tale funzione è assicurata da personale adeguatamente formato in modalità continua e specifica, che collabora con il Delegato del trattamento e con il Data Protection Officer per l'eliminazione ed il contenimento delle criticità relative alla gestione e protezione dell'informazione.

Il Facilitatore Privacy di struttura è individuato e nominato dal Delegato del trattamento dei dati e la comunicazione di tale nomina viene trasmessa al Data Protection Officer.

Il Data Protection Officer attiva il Registro dei Facilitatori privacy di struttura e si avvale di tali collaboratori per ricevere le informazioni necessarie all ' aggiorn am ent o continuo del Registro delle attività di trattamento dei dati personali e veicolare le indicazioni operative del Titolare del trattamento.

Articolo 19 - L' informativa all'Interessato

L' ASP adotta un sistema di documenti relative alle informazioni sul trattamento dei dati personali chiare e comprensibili all'utenza per fornire all'interessato tutte le notizia relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
Le informazioni sul trattamento dei dati personali riportano:

- l'identità e i dati di contatto del Titolare del trattamento e i dati di contatto, del Data Protection Officer;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le modalità di trattamento dei dati personali;
- obbligatorietà o meno del conferimento dei dati;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- come possono essere esercitati i diritti di accesso in base alle disposizioni vigenti;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica del trattamento che lo riguarda o di opporsi al loro trattamento;

- qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio di consenso al trattamento il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo al Garante;
- se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure è un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, le indicazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato;
- nel caso in cui i dati personali non siano stati ottenuti presso l'Interessato a questi deve essere resa nota la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

L'ASP predispone ulteriori informazioni specifiche, avvalendosi del Data Protection Officer e del Gruppo di lavoro Privacy, che rappresentano gli ulteriori e particolari trattamenti di dati da questa svolti.

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 con il Data Protection Officer .

L'ASP attiva, utilizzando diversi canali di comunicazione quali e-mail, home page, il link dedicato "Protezione dati personali" e sistemi Internet in genere, adeguate modalità di visibilità delle azioni poste in essere all'interno del!'ASP aziendali in attuazione della normativa sulla riservatezza dei dati.

Le informazioni sul trattamento dei dati personali non sono 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 20 - I diritti dell'Interessato

Gli interessati possono contattare il Data Protection Officer per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.
L'Interessato ha il diritto di ottenere dall' 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 dest i nat ari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d. il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e. l'esistenza del diritto di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali, laddove consent it a, 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 Privacy;
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, com presa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento.

L'Interessato ha il diritto di ottenere dall'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 al Data Protection Officer.

Il Data Protection Officer, avvia il procedimento, avvalendosi necessariamente dell'apporto e della collaborazione del Delegato del trattamento dei dati di competenza e 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 di cui al comma 1 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 21 - Diritto di opposizione

L'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano e I' 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 per l'esecuzione di un compito di interesse pubblico.

Articolo 22 - 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 documenti.

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 23 - 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 delegata, salvo il caso dei documenti relativi a dati regolati da normative speciali che prevedono il ritiro diretto dell' interessato.

Articolo 24 - La comunicazione dei dati personali all'esterno (destinatari)

La comunicazione dei dati personali all'esterno dell'ASP 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 di cui al precedente art. 5;
- qualora la comunicazione di dati personali ad altro soggetto pubblico che non sia prevista da normativa vigente e sia effettuata solo se prevista dal Regolamento per il Trattamento dei Dati Personali Sensibili e Giudiziari il cui schema tipo è stato approvato dal Garante, ovvero previa comunicazione alla stessa Autorità.

La suindicata trasmissione dei dati personali avviene in forma scritta o telematica

Articolo 25 - Le informazioni sullo stato di salute dell'interessato

I dati personali inerenti la salute possono essere comunicati all'Interessato o a soggetto da questi autorizzato, solo dal personale 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 designata.

A tal fine I'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.

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 26 - 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 sia effettuata soltanto nei limiti del principio di necessità, osservando le disposizioni del presente regolamento e delle relative misure di sicurezza.

Articolo 27- La diffusione dei dati personali e sensibili

La diffusione dei dati personali e sensibili in ambito aziendale è consentita soltanto per adempiere ad obblighi previsti dalle normative vigenti e nelle forme da queste previste, in particolare per quanto riguarda l'obbligo di trasparenza al quale è soggetta l' amministrazione.
La diffusione di qualsiasi dato di salute è comunque assolutamente vietata.

Articolo 28 - 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.

A riguardo I' 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.

Articolo 29 - 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 I' ASP il Sistema gestionale privacy è un requisito indispensabile di qualità per assicurare il quale adotta tutte le misure tecniche ed organizzative necessarie a far sì che la protezione dei dati personali e la loro tenuta in sicurezza siano non solo il rispetto di un obbligo normativo ma anche l'occasione di una crescita organizzativa e culturale capace di innovare I'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 stesso le 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 precontrattuale, 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 30 - La Valutazione di Impatto sulla protezione dei dati e la consultazione preventiva con l'Autorità Garante della protezione dei dati

L'ASP prima di attivare un trattamento dei dati personali si assicura che sia effettuata una apposita valutazione preliminare dell'impatto delle operazioni di trattamento, avvalendosi e consultandosi, qualora necessario, con il proprio Data Protection Officer.

La Valutazione di Impatto preliminare viene effettuata 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 la conformità 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 trasmessa al Data Protection Officer e la conserva all'interno del Sistema gestione privacy aziendale.

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 I' ASP, prima di procedere al trattamento, consulta l'Autorità Garante Privacy.

L'ASP, inoltre, attiva tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche individuate dall'Autorità Garante Privacy 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 31- Le misure di sicurezza

L'ASP e i Delegati del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura di sicurezza necessaria per assicurare un livello sufficiente di sicurezza dei dati personali trattati.

Questi, 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, mettono in atto misure tecniche e organizzative adeguate per 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 procedura informatica è consentito solo se congruente con il trattamento di dati per il quale il collaboratore dell'ASP è stato precedentemente designato Incaricato del trattamento ed è consentito soltanto utilizzando apposite credenziali di autorizzazione composte da un user-id, attribuito dall'Amministratore di Sistema di competenza e da una password .

La richiesta di rilascio delle credenziali per accedere alla procedura informatica , una volta sottoscritta dal Delegato del trattamento, è inoltrata all'Amministratore di Sistema di competenza che, una volta attribuite le relative credenziali, le custodisce presso il Servizio Informativo aziendale.

Il Data Protection Officer verifica, periodicamente in sede di audit, la congruenza della nomina ad incaricato 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 Incaricato del trattamento dei dati personali.

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

Spetta alla Direzione risorse umane comunicare al Data Protection Officer e all'Amministratore di Sistema gli aggiornamenti e le variazioni relative al personale (cessazioni, sost it uzi oni, 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 per 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 del trattamento degli Autorizzati ed Amministratori di Sistema al fine di un utilizzo consapevole delle informazioni;
- evidenzia le misure che I' ASP ha adottato nel tempo per proteggere i dati personali a sua disposizione e il piano delle azioni di miglioramento che intende adottare per l'anno in corso.

Il DAVR è predisposto dal Data Protection Officer con il supporto del Servizio Informatico aziendale al quale resta in carico fornire e produrre tutte le informazioni e documentazioni afferenti specificamente il predetto Servizio Informatico, tali da consentire al Data Protection Officer la produzione del documento in oggetto corredato dalle specifiche misure tecniche e organizzative adeguate.

Entro il 31 gennaio di ogni anno i Delegati e Responsabili del trattamento dei dati devono inviare al Data Protection Officer 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 32 - Le misure di sicurezza per i trattamenti di dati personali affidati a soggetti esterni

Responsabili e Sub - Responsabili esterni del trattamento sono tenuti ad assicurare al Titolare del trattamento di aver adottato, prima di effettuare attività di trattamento di dati, ogni misura minima di sicurezza prevista 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 altra misura idonea alla protezione dei dati loro affidati.

Tali responsabili sono tenuti ad inviare al Data Protection Officer, entro il 31 gennaio di ogni anno, 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 al riguardo 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 del trattamento 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 minime di sicurezza e non aver affidato alcune fasi del trattamento a soggetti terzi salvo che I' ASP non abbia autorizzato la nomina di questi come Sub-responsabile del trattamento dei dati personali.

A tale proposito, è fatto obbligo al Responsabile del Servizio Informatico aziendale di acquisire da parte del Responsabile del trattamento specifica attestazione circa la corretta adozione di misure tecniche ed organizzative regolarmente aggiornate e conformi agli ultimi standard

Qualora il Responsabile del trattamento utilizzi, al contrario , strumenti informatici forniti dall'ASP è tenuto a trasmettere copia degli atti di designazione a Autorizzati al Data Protection Officer che provvederà ad attivare le procedure necessarie al rilascio delle relative credenziali di accesso .

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

Articolo 33 - Gli interventi tecnici a cura di soggetti esterni

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

Articolo 34 - La tenuta in sicurezza dei documenti e archivi di titolarità dell'ASP

Gli archivi che custodiscono i dati di cui è titolare del trattamento I'ASP, cartacei e digitali, devono essere collocati in locali nari 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.

li Delegato del Trattamento attiva, attenendosi alle indicazioni del Data Protection Officer ed alle disposizioni e Procedure Aziendali vigenti, i criteri necessari a garantire accesso controllato ai locali ed accesso selezionato ai dati mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario di servizio 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 del trattamento.

Relativamente agli archivi digitali il rilascio di tale autorizzazione è di competenza dell'Amministratore di Sistema, previa indicazione del Delegato del Trattamento e comunicazione al Data Protection Officer.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Delegato del trattamento dei dati di competenza, che deve assicurare 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 I'ASP predispone un piano di scarto d'archivio, approvato con apposita deliberazione.

Relativamente agli archivi informatizzati di dati e di esclusiva pertinenza del Servizio Informatico aziendale, I' ASP adotta, facendo seguito alle disposizioni vigenti secondo standard e norme in tema di protezione dati e amministrazione digitale, in stretta collaborazione con i Delegati ed i Responsabili del trattamento dei dati e degli Amministratori di Sistema, idonee procedure di:

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

Resta obbligatorio da parte di qualunque dei suddetti soggetti segnalare eventuali criticità e problematiche al Titolare ed al Data Protection Officer.

Articolo 35 - I limiti alla conservazione dei dati personali

L'ASP assicura l'adozione di apposite misure e procedure attraverso le quali:

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

Articolo 36 - 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 trattamento dei dati da parte dei delegati , Responsabili, Sub-Responsabili, Amministratori di Sistema e Incaricati del trattamento.

I controlli e le verifiche sono effettuati previa programmazione periodica o in caso di necessità anche su sollecitazione degli interessati e le relative attività sono svolte dal personale a ciò incaricato sotto il coordinamento del Data Protection Officer.

Articolo 37- La formazione dei 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 del trattamento, degli Autorizzati da questi coordinati, degli Amministratori di Sistema e del personale di nuova assunzione sui temi della protezione dei dati personali e sui diritti, doveri ed adempimenti previsti dalla normativa vigente.

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

I Responsabili e dei Sub-Responsabili esterni del trattamento sono tenuti ad 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 38 - La violazione dei dati personali (concetti base con riferimento alla procedura aziendale del data-breach)

Ogni Responsabile, Delegato o Incaricato del trattamento dei dati personali è tenuto a informare senza ingiustificato ritardo il Titolare o il Data Protection Officer, del possibile caso di una violazione dei dati personali (cfr. "Procedura per la gestione dei Data Breach, adottata con deliberazione n.10/2018)

Ogni interessato, utilizzando l'apposito indirizzo mail può segnalare al Titolare (direzione.generale@asp.sr.it), al Data Protection Officer (rdp@asp.rg.it), un possibile caso di una violazione dei dati personali.

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

L'ASP provvede a notificare attraverso il Data Protection Officer la violazione all'Autorità Garante Privacy senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.

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

La notifica della violazione dei dati personali deve almeno:

- 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;
- 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;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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 39 - La disciplina delle misure del Regolamento

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

L'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 40 - 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 qualora per motivi organizzativi e/o la normativa e le direttive sopra citate lo rendano opportuno.