Azienda Pubblica di Servizi alla Persona
Pio Istituto Elemosiniere - Albertone Del Colle

REGOLAMENTO AZIENDALE SUL TRATTAMENTO DEI DATI PERSONALI

APPROVATO CON DECRETO DEL PRESIDENTE N. 1 DEL 13.02.2024

INDICE

PREMESSE

L'Azienda pubblica di servizi alla persona PIO ISTITUTO ELEMOSINIERE – A. DEL COLLE" ha intrapreso un percorso di progressiva riorganizzazione ed informatizzazione di tutti i procedimenti amministrativi aziendali, all'interno del quale acquista particolare rilievo il loro adeguamento alla normativa in materia di protezione dei dati personali (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» - di seguito GDPR), il quale - definitivamente vincolante a partire dal 25 maggio 2016 uniforma la normativa in tutti gli Stati Membri dell'Unione Europea e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, imponendo la previsione ed il rispetto di requisiti, adempimenti formali e misure di sicurezza volti a garantire la tutela dei diritti dell'interessato.

Il presente sistema di gestione dei dati personali comporta pertanto una serie di norme, restrizioni e controlli volti a garantire la sicurezza dei processi aziendali e definire le responsabilità degli utilizzatori delle risorse nel rispetto della normativa sulla privacy, al fine di:

- conseguire i migliori risultati nel proteggere le informazioni e i dati gestiti nell'ambito delle proprie attività da tutte le minacce interne o esterne, intenzionali o accidentali, secondo le disposizioni previste dalla normativa comunitaria e nazionale;
- garantire la riservatezza delle informazioni ed il corretto trattamento dei dati personali;
- assicurare la massima efficienza delle risorse informatiche ed il rispetto delle leggi in materia di utilizzo delle stesse;
- responsabilizzare e formare gli operatori circa i rischi penali, civili, amministrativi connessi all'uso indebito dei mezzi informatici;
- evitare che i propri operatori, utilizzando gli strumenti informatici dell'Azienda, compiano abusi legati all'utilizzo improprio delle risorse della rete Internet e della rete interna e dei dati ivi contenuti.

L'Azienda individua come elementi fondamentali delle politiche di protezione dei dati personali:

- la rilevazione e l'analisi dei trattamenti di dati personali, in modo da individuarne la tipologia nonché l'area organizzativa e ogni altro elemento necessario ad individuare le responsabilità relative al loro trattamento;
- la distribuzione dei compiti e delle responsabilità attribuite a coloro che trattano dati personali.

L'Azienda in considerazione dell'estrema delicatezza dei dati personali che tratta costantemente, della loro molteplicità e della numerosità dei soggetti che necessariamente devono trattarli, mette in atto tutte le misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali viene effettuato in conformità alla normativa vigente, con modalità tali da preservarne l'integrità e la confidenzialità.
L'attuazione del presente sistema compete a tutto il personale e si applica a tutti gli organi e alle strutture di qualsiasi livello organizzativo o funzionale.
Le misure sono riesaminate e aggiornate periodicamente
Le misure tecniche e organizzative qui individuate attuano i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e di protezione per impostazione predefinita (*privacy by default*) di cui all'art. 25 del GDPR.
L'inosservanza delle norme sulla privacy può comportare responsabilità di natura civile e penale per le persone che trattano dati personali raccolti dall'Asp Pio Istituto Elemosiniere – A. del Colle.

Il sistema di protezione dei dati si avvale dei seguenti soggetti, documenti, e sistemi organizzativi:

a) Registro delle attività di trattamento (che presuppone la mappatura dei trattamenti e l'identificazione dei ruoli "privacy" dei soggetti coinvolti);
b) Responsabile della Protezione dei Dati (RDP);
c) sistema di attribuzione delle responsabilità del trattamento dei dati personali;
d) documentazione relativa alle informative ed al rilascio delle nomine degli autorizzati al trattamento dei dati;
e) designazioni a specifici incarichi ex art. 2-quaterdecies del Codice privacy (es. amministratore di sistema, delegato privacy interno, autorizzato/a ad accedere alle immagini di un impianto di videosorveglianza…);
f) modulistica per la raccolta dei consensi;
g) analisi e valutazione dei rischi di trattamento e le valutazioni di impatto - DPIA;
h) regolamentazioni, procedure e disposizioni operative adottate per i singoli trattamenti di dati personali, regolamento per l'utilizzo delle risorse hardware e software dell'organizzazione;
i) sistema di verifica periodica del corretto trattamento dei dati personali;
j) sistema di formazione continua delle persone autorizzate, dei responsabili e degli amministratori di sistema;

k) procedure per l'esercizio dei diritti degli interessati;
l) procedure per la gestione delle violazioni dei dati personali.

Al fine di facilitare la lettura del documento, si riprendono le definizioni più rilevanti, tra quelle elencate all'art. 4 o in altri articoli del GDPR:

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.
Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute (o Dati sanitari): 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.
Particolari categorie di dati: dati personali che rivelino 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 sessuale o all'orientamento sessuale della persona (art. 9 del GDPR).
Dati personali relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le
preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
Pseudoanonimizzazione: 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;
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;
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;
Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del titolare del trattamento.
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
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.

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.
Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
Violazione dei dati personali - Data breach: Violazione di sicurezza che comporti 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.
Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro. In Italia, detta autorità è stata istituita nel "Garante per la protezione dei dati personali" dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101, che ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51).

Di seguito ulteriori definizioni desumibili dal Codice:
Responsabile della protezione dei dati - RPD: persona fisica, designata obbligatoriamente nei casi di cui all'art. 37 del GDPR 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;
Persone autorizzate al trattamento: le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento sotto la diretta autorità del Titolare o del Responsabile.
Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

PARTE PRIMA
FINALITÀ' E PRINCIPI

Articolo 1
Finalità

Il presente Regolamento disciplina il trattamento dei dati personali raccolti presso l'Azienda pubblica di servizi alla persona Pio Istituto Elemosiniere – A. del Colle, di seguito denominata Azienda, nel rispetto di quanto previsto dal D.lgs. n.196 del 30.06.2003 e successive modificazioni e dal Regolamento (UE) 2016/679 (General Data Protection Regulation), di seguito denominato GDPR.

Articolo 2
Oggetto del trattamento

Sono oggetto di trattamento qualsiasi informazione riguardante una persona fisica identificata o identificabile direttamente o indirettamente attraverso il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Per trattamento si intende 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.

Articolo 3
Principi per il trattamento dei dati personali

I dati vengono trattati nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'interessato nonché degli obblighi di correttezza, liceità e trasparenza imposti dal D.lgs. n.196 del 30.06.2003 e successive modificazioni e dal Regolamento UE 2016/679 GDPR.
La finalità e la base giuridica del trattamento, cui sono destinati i trattamenti dei dati personali rientrano nei compiti istituzionale dell'Azienda e riguardano in particolare:

1. l'esercizio delle funzioni amministrative e fiscali che riguardano gli Ospiti/Clienti;
2. la gestione dei dati socio-sanitari contenuti nelle cartelle individuali degli Ospiti/Clienti;
3. la gestione dei dati anagrafici dei famigliari degli utenti ai fini delle attività amministrative;
4. la gestione delle rilevazioni statistiche al fine di ottimizzare l'efficienza organizzativa;
5. la programmazione e pianificazione/esecuzione delle attività di animazione e socializzazione;
6. l'erogazione di prestazioni e interventi, socio-assistenziali e socio-sanitari ed attività amministrative connesse.

L'Azienda si impegna a garantire sempre la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività, trattandoli in conformità alle leggi vigenti in materia e secondo quanto disciplinato in questo Regolamento.
Il trattamento dei dati può essere effettuato attraverso strumenti manuali, informatici e telematici atti a memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste.
Tutti i soggetti in qualsiasi modo coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2407 del Codice civile. Tali obblighi di mantenimento del segreto professionale, della riservatezza, del divieto di comunicazione e/o diffusione permangono anche dopo la cessazione o la modifica dell'incarico.
Al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, ogni Persona Autorizzata deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie dall'Azienda per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando

tutti i dati confidenziali e soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- non devono essere eseguite operazioni di trattamento per fini non previsti dai compiti assegnati;
- devono essere svolte le sole operazioni di trattamento necessarie al raggiungimento dei fini per i quali i dati sono stati raccolti;
- deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Le succitate regole impongono, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed alla eventuale distruzione.
I dati raccolti dall'Azienda possono essere oggetto di conservazione sia analogica che digitale solo per il tempo previsto dalla normativa vigente e successivamente sono sottoposti a scarto d'archivio o distruzione.

Articolo 4
Campo di applicazione

Le disposizioni di cui al presente regolamento a; più nel dettaglio le disposizioni di cui al presente sistema si applicano a:
- tutte le persone fisiche che a qualsiasi titolo collaborano con l'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori dipendenti, lavoratori di operatori economici aggiudicatari di contratti pubblici, collaboratori a progetto, stagisti, consulenti, ecc., di seguito "persone autorizzate") e che si trovino ad operare sui dati aziendali e più specificatamente sui dati personali e dati sanitari mediante l'uso di strumenti informatici e di documenti analogici dei quali l'Azienda è titolare. Tali soggetti sono specificamente e formalmente autorizzati, e ritenuti responsabili, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza;
- tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda, a prescindere dall'esistenza di autorizzazione formale, relativamente a quanto pervenga a loro conoscenza nell'ambito del rapporto che intrattengono con l'Azienda e che devono garantire il rispetto dei requisiti contenuti nel presente Regolamento.

Articolo 5
Il sistema aziendale di protezione dei dati

Il sistema di protezione dei dati si avvale dei seguenti soggetti, documenti, e sistemi organizzativi:
a) Registro delle attività di trattamento (che presuppone la mappatura dei trattamenti e l'identificazione dei ruoli "privacy" dei soggetti coinvolti);
b) Responsabile della Protezione dei Dati (RDP);
c) sistema di attribuzione delle responsabilità del trattamento dei dati personali;
d) documentazione relativa alle informative ed al rilascio delle nomine degli autorizzati al trattamento dei dati;
e) designazioni a specifici incarichi ex art. 2-quaterdecies del Codice (es. amministratore di sistema, delegato privacy interno, autorizzato/a ad accedere alle immagini di un impianto di videosorveglianza…);
f) modulistica per la raccolta dei consensi;
g) analisi e valutazione dei rischi di trattamento e le valutazioni di impatto - DPIA;
h) regolamentazioni, le procedure e disposizioni operative adottate per i singoli trattamenti di dati personali regolamento per l'utilizzo delle risorse hardware e software dell'organizzazione;
i) sistema di verifica periodica del corretto trattamento dei dati personali;
j) sistema di formazione continua delle persone autorizzate, dei responsabili e degli amministratori di sistema;
k) procedure per l'esercizio dei diritti degli interessati;
l) procedure per la gestione delle violazioni dei dati personali.

PARTE SECONDA
SOGGETTI E RESPONSABILITÀ IN MATERIA DI TRATTAMENTO

Articolo 6
Titolare del trattamento

Il Titolare del trattamento dei dati personali è l'Azienda pubblica di servizi alla persona Pio Istituto Elemosiniere A. del Colle, rappresentata per la specifica materia dal Presidente del Consiglio d'amministrazione e legale rappresentante pro-tempore.
Ai sensi dell'articolo 24 del Regolamento UE 2016/679 GDPR (General Data Protection Regulation), il Titolare del trattamento è tenuto in particolare a:

- mettere in atto le misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (privacy by design) e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente
- garantire la riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- designare il responsabile del trattamento a cui affidare mansioni importanti e di elevata professionalità, in fase di gestione dei dati personali;
- designare gli incaricati del trattamento tra le persone dell'organizzazione aziendale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza.

Quando le finalità e i mezzi del trattamento di certi dati debbano essere determinati congiuntamente ad altri Titolari del trattamento, questi ultimi assumono 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 ed e i loro rapporti con gli Interessati, i quali possono conoscerne il contenuto ed esercitare i propri diritti nei confronti di e contro ciascun Titolare del trattamento.

Articolo 7
Responsabile della protezione dei dati o Data Protection Officer

L'Azienda individua il Responsabile della protezione dei dati ex art. 37 GDPR facendo esclusivo riferimento alle qualità professionali, alla conoscenza specialistica della normativa e delle prassi aziendali in materia di protezione dei dati e alla capacità di assolvere ai compiti individuati dalla normativa vigente.
L'incarico è affidato in forza della stipulazione di un contratto di servizi di norma di durata triennale che preveda espressamente lo svolgimento in piena autonomia e indipendenza, dei compiti e delle funzioni di cui all'art. 39 par. 1 del GDPR.
In seguito alla designazione, l'Azienda si fa carico di notificare al Garante il nominativo ed i punti di contatto del RDP, di provvedere alle relative pubblicazioni sul sito istituzionale e di farne menzione in tutte le informative consegnate alle persone fisiche e/o giuridiche di cui l'Azienda tratta dati personali.
L'Azienda assicura che il RDP 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.

Articolo 8
Responsabili del trattamento dei dati personali

L'Azienda designa come Responsabili del trattamento dei dati personali tutti i soggetti esterni cui sono delegate attività di competenza aziendale o attività connesse, qualora comportino necessariamente il trattamento dei dati personali.
Le attività di trattamento dei dati personali affidate ai soggetti esterni sono disciplinate con un apposito contratto, che vincola il Responsabile e l'eventuale Sub-Responsabile, 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 e sottoscritto in modalità digitale, prevede, in particolare, che il Responsabile del

trattamento:

a) tratti i dati personali osservando le procedure in materia di protezione dei dati personali adottate dal Titolare;
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'Azienda 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 l'Azienda con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato e di garantire il rispetto degli obblighi di legge, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
e) su indicazione dell'Azienda, cancelli o 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'Azienda 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.

I Responsabili del trattamento devono:

- osservare le procedure in materia di protezione dei dati personali adottate dal Titolare del trattamento;
- organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice;
- adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice e dal Regolamento e la conformità nel tempo dei sistemi e delle misure di sicurezza;
- redigere e aggiornare il registro delle attività di trattamento, qualora necessario;
- informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;
- nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;
- proporre al Titolare del trattamento dei dati la nomina di soggetti per il ruolo di sub-Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;
- attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore inoltrando al Titolare del trattamento le richieste pervenute nel caso non possano essere evase autonomamente;
- distruggere i dati personali alla fine del trattamento nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari;
- comunicare immediatamente al titolare non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;

In tutti gli atti che disciplinano rapporti con i soggetti di cui al precedente articolo (contratti, convenzioni, disciplinari di incarico, conferimenti, etc.), deve inoltre essere inserita l'indicazione che l'Azienda 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.

Il Titolare del trattamento è in ogni caso 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 9
Sub-responsabili del trattamento dei dati personali

I Responsabili possono delegare in tutto o in parte i trattamenti di dati personali che gli sono stati affidati ad altri soggetti denominati Sub-Responsabili del trattamento, purché sia stata rilasciata preventiva e specifica autorizzazione scritta dell'Azienda.
Nel caso in cui un Responsabile del trattamento ricorra a un Sub Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'Azienda, a tale altro soggetto sono imposti, mediante un contratto, gli stessi obblighi a cui è stato sottoposto il Responsabile.
Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti dell'Azienda l'intera responsabilità dell'adempimento degli obblighi del Sub-Responsabile.

Articolo 10
Delegati del trattamento dei dati personali e relativi compiti

Il Titolare del trattamento designa con apposito atto formale i Delegati del trattamento dei dati personali cui assegnare il coordinamento delle attività di trattamento dei dati, mediante specifiche indicazioni operative per il corretto assolvimento dei compiti. Tali nomine indicano i trattamenti di dati dei quali viene conferita la responsabilità del coordinamento, sono conservate presso l'Ufficio di Direzione Generale e sono comunicate al RDP.
L'Azienda designa quali Delegati 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.
La funzione di Delegato del trattamento dei dati personali è attribuita personalmente e non è suscettibile di ulteriore delega.
I Delegati:

- si attengono agli obblighi individuati dalla normativa vigente e dal presente sistema e, più specificamente, ai compiti e alle istruzioni notificati anche unitamente alla comunicazione della nomina;
- non possono trattare i dati personali se non sono previamente istruiti in tal senso dal Titolare;
- rilasciano all'interessato l'informativa e acquisiscono il consenso laddove necessario, secondo le istruzioni impartite dal Titolare del trattamento (o del Responsabile del trattamento di riferimento)
- designano formalmente le persone autorizzate al 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;
- mettono a disposizione dell'Azienda 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 RDP qualora un'istruzione ricevuta violi il presente Sistema o altre disposizioni vigenti relative alla protezione dei dati personali, inviando un'apposita comunicazione all'indirizzo mail del RDP;
- 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 tutte le disposizioni relative alle misure di sicurezza adottate dall'Azienda, le ulteriori linee guida sulla riservatezza dei dati, la protezione delle informazioni e sull'amministrazione digitale;
- hanno il compito di 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 RDP eventuali situazioni di potenziale compromissione della protezione dei dati personali;
- relativamente alla propria area 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 RDP su come svolgono i compiti specifici loro assegnati e segnalano appena possibile ogni problematica di riferimento.

Articolo 11
Persone autorizzate al trattamento dei dati personali

Le Persone autorizzate al trattamento dei dati personali (anche definite Incaricati) sono le persone fisiche che

effettuano le operazioni di trattamento di dati personali, autorizzati e designati a tale scopo dal Delegato o dal Responsabile del trattamento dei dati personali, 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.
Il soggetto autorizzato effettua tutte le operazioni di trattamento dei dati personali attinenti all'attività lavorativa di competenza dell'area di appartenenza e opera sotto l'autorità del Delegato (o del Responsabile del Trattamento), attenendosi alle istruzioni dallo stesso impartite nonché alle specifiche procedure che regolamentano le modalità di utilizzo delle banche dati cui lo stesso abbia accesso.
Gli Incaricati del trattamento dei dati personali:

- trattano i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza;
- sono personalmente responsabili della gestione riservata della password loro assegnata, ed è fatto loro assoluto divieto di cedere le proprie credenziali ad altri;
- sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento e hanno l'obbligo di restituirli al termine delle operazioni affidate;
- segnalano al Titolare o al Delegato, eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti;
- avvisano il Titolare o il Delegato qualora, nello svolgimento di un'attività, riscontrino il trattamento di nuovi dati e finalità per cui risultasse necessario aggiornare il registro dei trattamenti ed eseguire almeno un'analisi dei rischi;
- informano immediatamente il Titolare qualora le istruzioni ricevute risultino non conformi alla normativa sulla protezione dai dati;
- segnalano al Titolare o Delegato eventuali accessi non autorizzati.

Sono da designare come Incaricati sia i dipendenti dell'Azienda 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 ed eventuale fine dell'attività all'interno della struttura ed indica i trattamenti di dati di cui sono autorizzati a svolgere le relative operazioni.
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 conservato presso l'Ufficio amministrativo in archivio accessibile al RDP. La data di cessazione dall'incarico è registrata sull'atto di designazione e comunicata al RDP.
I Responsabili e/o Sub-Responsabili devono designare quali Incaricati i propri dipendenti e i collaboratori che, a qualsiasi titolo, prestino la loro opera, anche in via temporanea, trattando dati per conto dell'Azienda. Tali Responsabili conservano presso la loro sede legale gli originali degli atti di designazione ad Incaricato del trattamento.

Articolo 12
Amministratore di Sistema

La figura professionale che in ambito informatico mantiene, configura e gestisce un sistema di elaborazione dati o sue componenti, ivi inclusi i sistemi software, le basi dati, reti e apparati di telecomunicazione di sicurezza è nominata Amministratore di Sistema.
La nomina ad Amministratore di Sistema avviene - previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza – con apposito atto del Titolare, il cui originale viene conservato presso l'Ufficio di Direzione Generale e comunicato al RDP, 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.
L'Amministratore di sistema ha i seguenti compiti e responsabilità:

- sovraintendere all'infrastruttura tecnologica aziendale (risorse di rete, computer, applicativi) al fine di garantirne una corretta ed efficiente utilizzazione;
- gestire la creazione, l'attivazione, la disattivazione, la modifica degli account di rete e dei relativi privilegi di accesso alle risorse, assegnati ad utenti specifici dell'organizzazione in base alle richieste presentate dai Delegati del trattamento di riferimento nella loro qualità di Direttori d'Area;

- installare e/o rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- svolgere regolari attività di controllo, amministrazione e backup sui dischi locali dei PC degli utenti e sulle unità di rete e procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete;
- utilizzare le credenziali di accesso di Amministratore del sistema per accedere, anche da remoto, ai dati od alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale attività, tuttavia, deve essere disposta per mezzo del Delegato e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto. Di ciò ne viene successivamente data informazione all'utente;
- nell'ambito delle responsabilità assegnate, effettuare periodici controlli e verifiche tecniche, in merito a quanto previsto dal presente Sistema;
- individuare i soggetti a cui affidare l'incarico di manutentore del sistema informativo aziendale, informando il Titolare del Trattamento e formalizzando per iscritto l'attribuzione dell'incarico, specificando i limiti dell'intervento e le manutenzioni richieste. Per manutenzione s'intende non soltanto l'intervento tecnico diretto ad eliminare eventuali avarie hardware, ma anche gli interventi volti alla ricostruzione di archivi che dovessero in qualche modo risultare danneggiati o corrotti oltre all'intervento tecnico diretto ad eliminare eventuali avarie al software di sistema e all'applicativo utilizzato.

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'Azienda, 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.

Articolo 13
Informazione e formazione del personale

L'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dall'Azienda anche e soprattutto grazie alla particolare attenzione risposta nei confronti della formazione del personale.
Ai soggetti affidatari dei servizi con elevata intensità di manodopera con mansioni sociosanitarie viene inoltre richiesta analoga attenzione.
Annualmente vengono infatti previste per tutto il personale operante in struttura, sia dipendente che non dipendente, iniziative formative in ambito privacy.
La formazione del personale sarà pianificata in modo da risultare efficace e documentabile e da trattare tutti gli aspetti specifici attinenti alla protezione dei dati.

PARTE TERZA
STRUMENTI PER IL TRATTAMENTO DEI DATI

Articolo 14
Trattamento di dati sensibili o di categorie particolari di dati

L'Azienda 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 (ad esclusione dei dati necessari per finalità di cura che si trattano senza necessità del consenso);
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.

Qualora il trattamento sia basato sul consenso, è compito dell'Azienda dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
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 15
Registro delle attività di trattamento

Il Registro delle attività di trattamento è un documento contenente le seguenti informazioni relative alle operazioni di trattamento svolte:

a. il nome ed i dati di contatto dell'Azienda, ai sensi del precedente art.4;
b. le finalità del trattamento;
c. la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e. l'eventuale trasferimento di dati personali verso un ente terzo;
f. ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

L'Azienda redige il Registro, con personale all'uopo incaricato, in forma cartacea o informatizzata e lo conserva presso gli uffici amministrativi.

Esso rappresenta un elemento di accountability, dal momento che risulta essere un valido strumento per fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile ai fini della valutazione o analisi del rischio.

Articolo 16
Informativa

L'informativa contiene tutte le informazioni che il Titolare del trattamento è tenuto a fornire al soggetto di cui deve trattare i dati personali e in particolare:

a. l'identità e i dati di contatto del Titolare del trattamento;

- **b.** i dati di contatto del Responsabile del trattamento e della protezione dei dati;
- **c.** le finalità del trattamento cui sono destinati i dati personali, nonché la base giuridica del trattamento;
- **d.** gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- **e.** il periodo di conservazione dei dati personali;
- **f.** l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- **g.** qualora il trattamento sia stato espresso per il consenso al trattamento dei dati personali per una o più specifiche finalità, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- **h.** il diritto di proporre reclamo a un'autorità di controllo;
- **i.** se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure 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 tal dati;
- **j.** l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art.22, paragrafi 1 e 4 del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato.

Qualora l'Azienda intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, dovrà fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Per assolvere all'obbligo di informazione previsto dall'articolo 13 del Regolamento (UE) 2016/679 in relazione ai dati personali forniti direttamente dell'interessato o dalle persone autorizzate l'Azienda ha predisposto l'informativa sul trattamento dei dati personali diversificata in relazione alla tipologia dei dati forniti nelle seguenti tipologie:

- Allegato 4 per il trattamento dei dati personali degli Ospiti/Clienti;
- Allegato 5 per il trattamento dei dati personali del personale dipendente;
- Allegato 6 per il trattamento dei dati personali dei diversi soggetti che svolgono, in accordo con i servizi territoriali competenti, all'interno dell'Azienda attività di tirocinio, volontariato, borsa lavoro, misure alternative alla pena, ecc.;

Nelle altre ipotesi di trattamento dei dati in sede di bandi di gara, contratti, convenzioni, bandi di concorso pubblico, segnalazioni di disservizio ecc,… sarà utilizzata la seguente informativa di massima, adattabile alla specifica fattispecie: "*Ai sensi del D.Lgs 196 del 30.06.2003 e del DPGR UE/679/2016, i dati personali, anche di natura sensibile e giudiziaria, forniti in relazione alla presente procedura, saranno trattati esclusivamente per le finalità di gestione della medesima e dell'eventuale rapporto contrattuale ad essa conseguente*".

Articolo 17
Consenso al trattamento dei dati

Il consenso è la libera manifestazione dell'interessato o dalle persone autorizzate ad acconsentire al trattamento dei suoi dati personali, dopo che è stato preventivamente informato tramite l'informativa di cui al precedente articolo 9.
Il consenso deve essere espresso mediante un atto positivo inequivocabile con il quale l'interessato o le altre persone autorizzate manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali.
Negli Allegati citati all'articolo 9 sono state previste le dichiarazioni scritte per consentire ai diversi soggetti di esprimere il proprio consenso al trattamento dei dati personali.

PARTE QUARTA
DATI E DIRITTI DELL'INTERESSATO

Articolo 18
I diritti dell'interessato

Il titolare si impegna a garantire a ciascun interessato i diritti tutelati dal GDPR e, nello specifico:

- il **diritto all'accesso**, cioè di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento (art. 15 GDPR);
- il **diritto di rettifica**, cioè di ottenere l'aggiornamento, la correzione ovvero l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa (art. 16 GDPR);
- il **diritto alla cancellazione**, cioè di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati (art. 17 GDPR);
- il **diritto all'opposizione**, cioè di limitare od opporsi, per motivi legittimi, al trattamento, seguendo le modalità descritte dalle norme vigenti. L'Azienda 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 (art. 21 GDPR).

Al fine di esercitare i diritti sopra descritti, l'Azienda si impegna a rispondere senza ritardo alle istanze presentate da parte dell'interessato direttamente al Titolare, ai Delegati, Responsabili, al RDP nelle forme e modalità nonché attraverso i mezzi ritenuti più idonei.
I suddetti diritti concernenti dati personali di 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.
L'Azienda, 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 detenuti dall'Azienda.
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, ai sensi dell'art. 24 della legge 241/1990.

Articolo 19
Accessibilità ai dati da parte di incaricati e persone autorizzate

Gli incaricati possono accedere esclusivamente a quei dati la cui conoscenza è strettamente necessaria per adempiere ai compiti affidati e indispensabili per l'esecuzione delle prestazioni aziendali.
Gli incaricati possono effettuare esclusivamente i trattamenti di dati personali definiti per lo specifico ruolo nella lettera di nomina, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea, degli strumenti informatici, e delle banche dati aziendali che contengono i già menzionati dati personali nei limiti di quanto previsto per lo specifico trattamento dallo specifico ruolo.
A ciascuna persona autorizzata è consentito accedere esclusivamente ai dati personali e sanitari dei pazienti in favore dei quali debba rendere la propria prestazione per finalità di assistenza, diagnosi e cura. È tassativamente vietato trattare i dati dei pazienti per finalità diverse da quelle sopra indicate e trattare dati di pazienti ospitati in altri Nuclei di degenza rispetto a quello di lavoro.
Accedendo ai dati sanitari, la persona autorizzata deve sempre prestare attenzione a che le altre persone presenti non possano visualizzare dati ai quali non sono autorizzati. Questo vale sia per i soggetti esterni (pazienti, visitatori, fornitori, ecc) sia per le altre persone interne non autorizzate per la funzione svolta o perché estranei al reparto o servizio. Occorre sempre porsi la domanda se la persona che visualizza i dati assieme a noi abbia titolo o meno per accedere ai dati.

Articolo 20

Le Informazioni sullo stato di salute dell'interessato

Le informazioni sullo stato di salute dei pazienti sono comunicate solo al paziente stesso (Interessato) o a soggetto da questo formalmente designato e che sia munito dei necessari poteri di rappresentanza (figli, amministratori di sostegno, tutori) e previo accertamento della sua identità. Nel caso il paziente lo abbia espressamene richiesto, i dati possono essere comunicati anche agli altri soggetti nominativamente indicati dal paziente (o da chi lo rappresenta) per lo specifico episodio di cura.
In relazione alla tipologia di informazione richiesta, la comunicazione è fatta dal solo personale medico quando riguarda diagnosi, valutazioni di esami clinici, lettura di referti medici specialistici, o anche dal personale infermieristico quando riguarda lo stato di salute in generale e le attività assistenziali e dal personale di riabilitazione riguardo al percorso riabilitativo intrapreso; l'eventuale comunicazione telefonica deve prevedere opportuni accorgimenti volti ad assicurare che le informazioni vengano date ai soli soggetti legittimati..
Il restante personale (assistenziale) non può rilasciare all'interessato informazioni sul suo stato di salute, a meno che non abbia ricevuto specifica delega in tal senso da parte del Titolare o del Responsabile del trattamento.
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.
Si deve sempre garantire il rispetto del segreto professionale connesso con la prestazione sanitaria e la diffusione di qualsiasi dato di salute è assolutamente vietata. Nessun dato personale e sanitario può essere comunicato o trasmesso a terzi se non per finalità istituzionali e solo nei casi espressamente previsti da specifiche procedure interne.
La copia della documentazione sanitaria richiesta dall'interessato o da un suo delegato viene consegnata in busta chiusa e può essere ritirata solo da tali soggetti.
La comunicazione dei dati personali all'esterno dell'Azienda è effettuata esclusivamente 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.

Articolo 21
Raccolta e riservatezza dei dati sanitari

La raccolta dei dati personali e sanitari ed i loro inserimento negli archivi aziendali è consentito solo dopo aver fornito al paziente l'informativa sul trattamento dei propri dati ed aver successivamente raccolto il suo consenso scritto al trattamento, fatta salva la necessità del loro utilizzo per finalità di cura. Sono comunque fatte salve le situazioni di emergenza sanitaria nelle quali il paziente non sia cosciente o non sia in grado di prestare il proprio consenso. In questi casi l'informativa dovrà essere resa ed il consenso raccolto non appena la situazione sanitaria del paziento lo dovesse consentire.
Le uniche finalità per le quali l'Azienda raccoglie i dati sanitari sono quelle di assistenza, diagnosi e cura. La persona autorizzata non può in nessun caso utilizzare i dati raccolti per finalità diverse.
La persona autorizzata che scambia informazioni di dati sanitari con altre persone autorizzate e/o con i pazienti stessi deve assicurarsi che non siano presenti altre persone esterne e non autorizzate; si deve utilizzare un tono di voce compatibile con le necessità di riservatezza.
La persona autorizzata deve inoltre prestare particolare attenzione all'inserimento dei dati personali e sanitari nei programmi che gestiscono i processi sanitari, verificando scrupolosamente la correttezza dei dati raccolti e deve inoltre:

- adottare tutte le misure di sicurezza concretamente necessarie a garantire la costante tutela della riservatezza dei dati sanitari dei pazienti;
- condividere i dati sanitari solo con le altre persone autorizzate direttamene coinvolte nel processo di assistenza, diagnosi e cura e condividere solo i dati strettamente necessari allo svolgimento delle attività di ciascuno in base al ruolo ricoperto in Azienda;
- evitare di dare o chiedere ad altre persone autorizzate informazioni sulle condizioni cliniche dei pazienti per mere esigenze informative personali;
- evitare di confrontarsi con le altre persone autorizzate sulle condizioni cliniche dei pazienti nei corridoi o in luoghi nei quali possano essere presenti persone interne non autorizzate o soggetti terzi;
- nel caso in cui il paziente condivida la camera con altri soggetti, effettuare i colloqui col paziente o con i suoi familiari se possibile in un luogo riservato e comunque nel modo più riservato possibile nelle specifiche condizioni logistiche;

- assicurarsi che pazienti o visitatori non entrino nelle sale riservate al personale dove sono custoditi dati personali e sanitari;
- assicurarsi che le persone interne estranee al nucleo di degenza non entrino nelle sale riservate al personale dove sono custoditi dati personali e sanitari.

Le persone autorizzate che per qualsiasi motivo dovessero trovarsi in luoghi della struttura nei quali siano presenti dati sanitari ai quali non sono autorizzati ad accedere, devono sempre mettersi nella condizione di non carpirli nemmeno per caso; non devono mai indugiare con lo sguardo su dati che fossero visibili su documenti cartacei o sullo schermo di un PC.
Gli schermi dei monitor dei PC fissi usati per accedere a dati sanitari devono essere sempre posizionati in modo da non essere visibili dall'esterno del locale che li ospita; i PC portatili ed i tablet utilizzati nei corridoi dei reparti per registrare i dati sanitari non devono mai essere lasciati incustoditi con i dati sanitari visibili.
Particolare attenzione deve essere prestata alla custodia e all'archiviazione delle cartelle sanitarie cartacee, dei referti clinici cartacei dei pazienti o di tutti i documenti stampati per la gestione dei processi sociosanitari (liste idratazioni, lista bagni, ecc.…), assicurandosi di non depositarli, neppure temporaneamente, in luoghi in cui rimangano incustoditi e nei quali possano accedervi soggetti terzi non autorizzati.
Non è consentito il trasferimento di dati personali oggetto di trattamento al di fuori del luogo di lavoro, né è consentita la rimozione di supporti cartacei contenenti dati personali di terzi senza autorizzazione.

Articolo 22
Comunicazione di dati sanitari a terzi e trasmissione di documenti

Si possono dare informazioni sullo stato di salute a soggetti diversi dall'interessato e dai suoi rappresentanti quando questi abbia manifestato uno specifico consenso, consenso che può essere manifestato anche da parte di un altro soggetto legittimato in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato.
In ogni caso le informazioni contenenti dati sanitari comunicate a terzi autorizzati devono essere quelle strettamente indispensabili per la gestione dell'episodio di cura del paziente e non per mere esigenze informative dell'interlocutore.
Anche la sola conferma della presenza di un paziente ospite presso la struttura è considerata un dato sanitario e non deve essere mai comunicato a terzi se non seguendo le regole dei paragrafi precedenti.
Le comunicazioni telefoniche di dati sanitari devono essere sempre ridotte ai casi strettamente indispensabili al processo di assistenza, diagnosi e cura e possono avvenire solo dopo essersi accertati sia dell'identità dell'interlocutore sia dell'esistenza di una specifica autorizzazione sullo specifico episodio di cura. Devono essere, ove possibile, privilegiate le comunicazioni di persona.
L'Azienda si pone come obiettivo la totale eliminazione della trasmissione o ricezione dei dati sanitari a mezzo fax. Per raggiungerlo ogni persona autorizzata deve sempre dissuadere l'interlocutore dall'utilizzo del fax quale mezzo di trasmissione di dati sanitari invitandolo sempre a fornire in alternativa un indirizzo di posta elettronica. I dati sanitari possono essere inviati via fax solo se l'interlocutore non dovesse realmente disporre di altri strumenti di comunicazione. Nel caso di invio occorre essere assolutamente certi del numero di telefono al quale il fax viene inviato, dell'identità della persona fisica che poi entrerà in possesso delle informazioni e, infine, del fatto che il soggetto destinatario sia autorizzato a conoscerle. Occorre sempre avere la ragionevole certezza che il fax al quale si inviano i documenti contenenti dati sanitari sia presidiato e che i documenti entrino in possesso solo ed esclusivamente della persona con la quale si intende interloquire. Nel caso di ricezione occorre chiedere all'interlocutore di essere avvertiti prima dell'invio dei documenti in modo da poter presidiare il fax e ritirare il documento non appena stampato.
Quando il dato sanitario deve essere inviato a mezzo posta elettronica occorre prestare la massima attenzione affinché l'indirizzo del destinatario sia corretto e gli eventuali file allegati siano quelli che realmente si intende inviare.
Nel caso si rendesse necessario l'invio tramite posta elettronica di schermate di applicativi software o di report a scopo di richiesta di assistenza, i dati presenti nell'immagine devono essere preventivamente anonimizzati cancellando sempre il nome e la data di nascita del paziente ed identificando i dati oggetto di assistenza mediante codice (numero impegnativa, numero di cartella clinica, ecc.)
I documenti contenenti dati sanitari (analisi di laboratorio, referti, documenti contenuti nella cartella clinica e foglio per le dimissioni SDO) – di norma in busta chiusa - possono essere consegnati a mano solo una volta accertata l'identità del soggetto richiedente, che deve coincidere col paziente interessato o un soggetto che lo assista e che sia munito dei necessari poteri di rappresentanza (genitori, amministratori di sostegno, tutori) o di apposita delega accompagnata da copia fotostatica del documento d'identità del delegante e del delegato.

Articolo 23
Campioni umani biologici

I campioni biologici umani sono a tutti gli effetti "dati particolari" e le regole di gestione sono le stesse previste per il trattamento dei dati sanitari.
Dal prelievo sino alla consegna al laboratorio analisi del Distretto Sanitario, i campioni biologici non devono mai restare incustoditi, neppure all'interno delle sale di medici e infermieri se queste sono accessibili a terzi. Il trasporto verso il laboratorio esterno deve avvenire in un contenitore che garantisca che i campioni ivi presenti non siano accessibili a soggetti terzi o comunque non autorizzati.

PARTE QUINTA
TRATTAMENTO DI DATI ATTRAVERSO LA RETE INFORMATICA AZIENDALE

Articolo 24
La Rete informatica aziendale

La rete informatica dell'Asp Pio Istituto Elemosiniere è costituita dalle risorse informatiche strutturali e dal patrimonio informativo digitale:

- le risorse informatiche sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica aziendale e componenti il sistema di trasmissione, ricezione ed elaborazione digitale del patrimonio informativo;
- il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

L'utilizzo della rete informatica è consentito solo al personale autorizzato e per l'esclusivo svolgimento delle proprie mansioni; l'accesso ai servizi informatici deve avvenire solo utilizzando le stazioni di lavoro (personal computer) e gli strumenti software messi a disposizione dall'Azienda esclusivamente con le proprie credenziali personali di autenticazione (userID e password).

Articolo 25
Creazione e gestione degli account e gestione delle Password

L'utilizzo delle risorse informatiche ai singoli incaricati è autorizzato dall'Amministratore di sistema, previa richiesta scritta da parte del Delegato nella sua qualità di Direttore d'Area (da inviarsi via mail) di creazione di un nuovo account (userID e password), con indicazione del profilo di autorizzazione per ogni applicativo/banca dati aziendale e/o per l'uso di servizi/programmi specifici richiesto, che provvede al rilascio di quanto richiesto.
Le credenziali di accesso sono strettamente personali, ovvero associate univocamente alla persona assegnataria, vanno custodite con diligenza e non devono mai essere comunicate ad altri compresi i propri superiori.
Dopo la prima comunicazione delle credenziali di autenticazione da parte dell'Amministratore, l'utente deve procedere a modificare la propria password al suo primo utilizzo, procedendo allo stesso modo ogni 180 giorni, ovvero tempestivamente in caso di sospetto di avvenuta conoscenza e divulgazione ad altri soggetti delle proprie password.
I requisiti minimi di complessità delle password sono:

- composizione con inclusione di caratteri maiuscoli e minuscoli, numeri, caratteri speciali e/o segni di punteggiatura;
- lunghezza non inferiore ad almeno 8 caratteri;
- password non agevolmente riconducibile all'identità del soggetto che la gestisce: evitare di includere parti del nome, cognome e/o comunque elementi agevolmente riconducibili all'utente, evitare l'utilizzo di password comuni e/o prevedibili.

L'utente è tenuto a custodire e garantire la segretezza della password ed è severamente vietato scriverla sul monitor, su post-it facilmente accessibili, o su altri supporti informatici non protetti da password (file txt, xls, doc), né deve essere lasciata memorizzata sul proprio PC.
La persona autorizzata non deve utilizzare credenziali di altre persone nemmeno se fornite volontariamente dal titolare delle stesse; nel caso in cui venga in qualsiasi modo a conoscenza delle credenziali di altri operatori, la Persona Autorizzata deve darne immediata comunicazione all'Amministratore che a sua volta imporrà il cambio password al titolare delle stesse.
Nel caso di smarrimento delle credenziali di accesso la Persona Autorizzata deve prontamente darne comunicazione all'Azienda che provvederà a cambiarle ed a comunicargliele nuovamente.
In caso di interruzione del rapporto di lavoro con il dipendente, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 30 giorni da quella data.
L'Amministratore del sistema annota in un apposito registro digitale l'elenco dei dipendenti ai quali è stato assegnato un nome utente, ed il tempo di utilizzo del medesimo.

Articolo 26
La postazione di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito, PC), notebook, accessori, periferiche ed ogni altro device concesso dall'Azienda in utilizzo all'utente.

Al fine di disciplinare un corretto utilizzo di tali beni, l'Azienda ha adottato le regole tecniche, che di seguito si riportano:

- ogni PC, notebook, accessori e periferiche incluse, sia esso acquistato o noleggiato, rimane di esclusiva proprietà dell'Azienda, ed è concesso all'utente ovvero al servizio/nucleo nel quale la persona autorizzata opera per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti le attività svolte;
- è dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
- gli accessi alle banche dati informatizzate e/o ai dati personali oggetto di trattamento dovranno avvenire solo tramite l'elaboratore/gli elaboratori assegnati, di cui l'utente è personalmente responsabile durante il periodo in cui svolge la prestazione lavorativa;
- l'utente dovrà evitare di divulgare ad altri la propria user-id e password e mettere in atto tutti gli strumenti e le precauzioni necessarie al fine di evitare l'accesso alla risorsa da parte di soggetti non autorizzati, ogniqualvolta ci si allontana dal personal computer (ad es. procedere al blocco del computer oppure all'attivazione automatica dello screen saver protetto da password);
- è vietato permettete ai colleghi, né tanto meno ad esterni, di operare sulla propria postazione di lavoro con le sue credenziali; diversamente si risulterà autore di qualunque azione;
- il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Azienda; per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa richiesta scritta dell'utente indirizzata al proprio Direttore d'Area, il quale ne valuterà i requisiti tecnici e l'aderenza alle policy interne ed al ruolo ricoperto in azienda;
- le postazioni di lavoro non devono essere lasciate incustodite con le applicazioni attive ed accessibili. A tal fine – quando ci si allontana dalla propria postazione di lavoro – si deve bloccare lo schermo con un programma salvaschermo (screensaver) protetto da password od effettuare il log-out (disconnessione) dalla sessione per gli applicativi utilizzati in cloud. Il personal computer deve essere spento al termine del suo utilizzo, in caso di assenze prolungate dall'ufficio ed in ogni caso sempre a fine della giornata lavorativa;
- l'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Delegato in qualità di Direttore d'Area eventuali minacce virus, guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature;
- l'Azienda si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata;
- è vietato:
  - il collegamento al proprio computer o alle reti informatiche aziendali, salvo preventiva autorizzazione scritta del Responsabile di riferimento, di apparecchi di proprietà personale, quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc.;
  - cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;
  - modificare la configurazione hardware e software del proprio PC, né collegare o scollegare le relative periferiche (stampati, scanner, mouse, tastiere, ecc), se non previa esplicita autorizzazione dell'Azienda che la esegue per mezzo dell'amministratore del sistema;
  - salvare sul PC file personali quali, a titolo di esempio, fotografie, file musicali, file video, file di attività extra lavorative;
  - rimuovere, danneggiare o asportare componenti hardware; modificare, le caratteristiche impostate sul PC assegnato, gli indirizzi IP, i punti rete di accesso e le configurazioni delle reti LAN/WAN configurate; attivare la password di accensione (bios) sul proprio PC;
  - installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Azienda. l'Azienda, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.
  - collegare al PC o utilizzare supporti removibili di origine sconosciuta (hard disk esterni, penne usb etc.). Ad esempio, non può assolutamente collegare al PC una chiavetta USB trovata per caso;
  - utilizzare risorse informatiche personali (PC, notebook, tablet, smartphone, ecc.) per accedere alla rete o ai dati aziendali a meno che non sia stato esplicitamente autorizzato. In tal caso anche per gli apparati personali la Persona Autorizzata deve attenersi alle stesse disposizioni previste per gli apparati aziendali;
  - memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

I dati personali e le altre informazioni dell'Utente che sono contenuti negli strumenti informatici aziendali e nei log reperibili nella memoria dei pc aziendali e sul server, sono registrati e potranno essere trattati per finalità di manutenzione hardware e software solamente in caso di necessità documentate dal Titolare.

Articolo 27
La Rete Locale Aziendale

L'accesso alla rete aziendale verrà specificamente autorizzato dall'Amministratore di sistema.
Ai Direttori (generale e d'Area) e ai loro collaboratori viene creata ed assegnata una cartella sul server (denominata con il "nome utente" dello stesso) per il salvataggio dei propri documenti di lavoro, sulla quale è garantita la creazione di copie di sicurezza (backup) ed è l'unico supporto sicuro sul quale memorizzare i documenti elettronici. Tale cartella – di norma – è disponibile agli altri utenti in modalità "sola lettura", ovvero in modalità "lettura e scrittura" se contenente informazioni gestite da più utenti. Qualsiasi file estraneo all'attività lavorativa, se non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato nelle cartelle di rete.
È assolutamente vietato salvare su disco locale (C:\) e sul desktop documenti riguardanti procedimenti ufficiali. Si ricorda che – in caso di file riservati – è possibile utilizzare – in sede di salvataggio del documento - una password per evitare l'apertura o la modifica di documenti da parte di persone non autorizzate.
Le cartelle della Persona Autorizzata o le cartelle di gruppo presenti nei server aziendali sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup, mentre tutti i dischi o altre unità di memorizzazione locali dei singoli PC non sono soggette a copie di sicurezza e pertanto non è garantita la sicurezza del dato in caso di guasti hardware, sovrascritture o cancellazioni accidentali, attacchi informatici di virus o altri software malevoli.

Articolo 28
Regole di archiviazione digitale

Al fine di non creare eccessivi appesantimenti sui dischi fissi del server e nelle copie di sicurezza riversate in cloud si prescrive di:

- non salvare permanentemente documenti PDF che sono stati o che verranno protocollati (e pertanto saranno accessibili mediante il Protocollo Informatico) o che comunque vengono registrati, ad esempio: preventivi, richieste di preventivi e simili; domande di accoglimento ed allegati; scansioni di atti ufficiali (delibere, determine, capitolati di gara e simili);
- evitare assolutamente la duplicazione di dati ed archiviazioni ridondanti: non creare sommariamente copie di cartelle per l'istruzione di procedimenti analoghi, ma copiare solamente i file utili, avendo cura di rinominarli correttamente;
- eliminare copie obsolete e versioni non ufficiali di file (ad es. "prova", "bozza", "vecchia", "OK", "1", "2"…): costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili;
- evitare di creare copie di file, copie di copie, … senza rinominarli correttamente.

E' buona regola inoltre:

- utilizzare nomi di salvataggio il più possibile chiari e che permettano la comprensione del contenuto;
- per il medesimo tipo di documento, salvare solo un documento "tipo" da utilizzare in tutti i casi di necessità di emissione di successivi atti analoghi, esempi: richiesta di preventivo, conferma preventivo, ordine di acquisto; comunicazioni derivanti da presentazione domande di accoglimento; contratto individuale di lavoro, lettera assunzione/ fine prova; dichiarazioni varie di contenuto analogo.

Non è consentito salvare documenti personali su nessuna risorsa hardware. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, potranno essere svolte regolari attività di controllo, amministrazione e **backup** da parte dell'Amministratore del sistema.
L'Azienda può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei dati sia sui singoli PC sia sulle unità di rete.

Articolo 29

Protezione antivirus

Il sistema informatico aziendale è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
Occorre sempre essere consapevoli che la posta elettronica e la navigazione Internet sono veicoli per l'introduzione sul proprio PC (e quindi nella rete aziendale) di virus e altri elementi potenzialmente dannosi. Questi strumenti vanno quindi sempre utilizzati con un adeguato livello di attenzione e nel rigoroso rispetto delle direttive impartite.
A tal fine, ogni utente è tenuto a:

- controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato;
- segnalare tempestivamente all'Amministratore di sistema eventuali avvisi di rischio ricevuti dal software antivirus installato o altre anomalie di funzionamento del sistema;
- evitare tassativamente l'apertura di file allegati ad e-mail provenienti da utenti sconosciuti o contenenti messaggi sospetti;
- evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile;
- evitare l'utilizzo di dispositivi rimuovibili (USB drive, CD/DVD, floppy disk o simili) personali o di provenienza ignota. Nel caso per lo svolgimento delle attività lavorativa si rendesse necessario l'utilizzo di supporti removibili (chiavette USB, Hard Disk esterni, CD, DVD), ogni Persona Autorizzata deve prestare la massima attenzione accertandosi preventivamente della provenienza del supporto stesso, effettuando sempre scansione antivirus prima di accedere al suo contenuto

Nel caso l'antivirus rilevi la presenza di un virus, segnalandolo con apposito messaggio, o si verifichi un malfunzionamento del PC, che possa far sospettare la presenza di un virus, la Persona Autorizzata deve:

- sospendere ogni operazione sul PC evitando di lavorare con il sistema infetto;
- informare immediatamente l'Amministratore di sistema.

Articolo 30
Utilizzo di dispositivi su supporti rimuovibili

Tutti i dispositivi rimovibili che consentono di copiare o archiviare dati, files, o documenti esternamente al computer (cd-rom, dvd, penne/chiavette/hard-disk usb, ecc.) contenenti dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da soggetti non autorizzati al trattamento dei relativi dati.
I supporti magnetici contenenti dati personali devono essere custoditi in archivi chiusi a chiave.
Non è consentito scaricare files contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa né utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'Azienda.
Tutti i supporti rimovibili di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo da parte dell'Amministratore di sistema.

Articolo 31
Utilizzo di PC Portatili, Tablet e smartphone aziendali

Ciascuno è responsabile degli strumenti di elaborazione e comunicazione portatili assegnatigli dall'Azienda (notebook, tablet e smartphone) e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro o altrove.
Al pari degli altri strumenti aziendali, anche gli strumenti portatili devono essere utilizzati solo per attività pertinenti rispetto allo svolgimento dell'attività lavorativa.
Al PC portatile si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
Non è consentito all'utilizzatore caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.
Il telefono aziendale affidato alla Persona Autorizzata è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, e non sono quindi consentite comunicazioni a carattere

personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità e urgenza.
Gli strumenti portatili non devono essere mai lasciati incustoditi in caso di utilizzo in ambito esterno all'Azienda e devono essere conservati in un luogo sicuro alla fine della giornata lavorativa.
In caso di furto o smarrimento dello strumento portatile aziendale deve esserne immediatamente notizia all'Amministratore di sistema.
La Persona Autorizzata deve prestare la massima attenzione alla rete utilizzata per connettere ad internet gli strumenti portatili aziendali: devono essere evitate sempre le reti WiFi pubbliche aperte e senza password di protezione; possono essere utilizzare reti WiFi protette personali o messe a disposizione da clienti o fornitori avendo cura di utilizzare solo connessioni criptate (HTTPS) per accedere ai dati aziendali.

Articolo 32
Utilizzo delle stampanti, multifunzione e fax

L'utilizzo delle stampanti presenti nel proprio ufficio, delle multifunzioni di rete, del fax e dei materiali di consumo in genere (carta, inchiostro, toner,) è riservato esclusivamente per finalità lavorative. E' buona regola evitare in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi, tenuto presente che per alcuni servizi è attivo il conteggio delle operazioni effettuate.
E' cura dell'utente effettuare la stampa o la fotocopiatura di documenti e dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
E' richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa. A tal fine è consigliabile impostare la cd. "stampa privata", in modo che da poter inviare il documento alla stampante ma di poterlo stampare solo previo sblocco dal pannello comandi, mediante un codice personale di 4/8 cifre.
L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

Articolo 33
Utilizzo della rete internet e dei relativi servizi

Il PC abilitato alla navigazione Internet assegnato alla singola persona autorizzata o al Servizio nel quale la persona autorizzata opera e costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
In questo senso, a titolo puramente esemplificativo, la persona autorizzata deve evitare:

- di navigare in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa;
- di scaricare e diffondere software gratuito (freeware), giochi, immagini e shareware prelevati da siti Internet, e non attinenti all'attività di servizio;
- di scaricare file multimediali (filmati e musica) per finalità non direttamente afferenti all'attività lavorativa, e previa verifica dell'attendibilità dei siti in questione;
- di navigare in siti - e scaricare documenti informatici - di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- di accedere a flussi in streaming video da Internet per scopi non istituzionali (ad esempio guardare video o filmati utilizzando le risorse Internet);
- ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- di procedere ad ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- di partecipare a forum o blog non professionali, di utilizzare chat line (esclusi gli strumenti autorizzati), bacheche elettroniche e registrazioni in guest books e social networks anche utilizzando pseudonimi (o nicknames), se non attinenti all'attività lavorativa svolta;
- di utilizzare sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.

L'Amministratore - al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti - si riserva la facoltà di applicare per singoli e/o gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con la Direzione, e di configurare specifici blocchi e/o filtri automatici che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

Articolo 34
Utilizzo della posta elettronica

Le caselle di posta elettronica sono uno strumento di lavoro e le persone assegnatarie sono responsabili del corretto utilizzo delle stesse.
Tutte le caselle appartenenti al dominio istituzionale @aspvenzone.it sono di esclusiva proprietà dell'Azienda e il loro utilizzo è autorizzato solo per l'esclusivo svolgimento delle mansioni lavorative affidate.
L'Azienda provvede ad assegnare una casella di posta elettronica personale (nome.cognome@aspvenzone.it) ad esclusivo e riservato utilizzo della singola persona autorizzata – e quindi non divulgabile al di fuori dell'Azienda - ed una o più caselle di posta elettronica cd. di servizio (es. amministrazione@aspvenzone.it) - anche condivise con altri utenti che afferiscono allo stesso servizio/nucleo/unità operativa – le quali sono le uniche caselle che devono essere utilizzate per la trasmissione ed il ricevimento di messaggi inerenti le attività del servizio/nucleo. Le credenziali di accesso non devono mai essere salvate su PC il cui uso è consentito a più persone.
Le caselle di posta elettronica (sia personali che di servizio) devono essere utilizzate solo per motivi strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, la persona autorizzata non potrà utilizzare la posta elettronica per:

- l'invio o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) o file in genere non legati all'attività lavorativa;
- l'invio o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche;
- iscriversi a newsletter, forum, blog, o servizi on line in genere non strettamente legati all'attività lavorativa.

Non è consentito fare uso della funzionalità di reindirizzamento della propria posta elettronica aziendale ad una casella di posta elettronica privata esterna.
L'accesso alla mail aziendale può avvenire utilizzando un software di posta elettronica (es. MS Outlook, Mozilla Thunderbird) oppure via web mail, mediante il PC aziendale.
La persona autorizzata nella formulazione dei messaggi deve sempre far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione dell'Azienda. Non devono essere predisposti messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.
Occorre prestare sempre la massima attenzione alle informazioni inviate via posta elettronica ed accertarsi che i destinatari della corrispondenza siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare; in caso di errore nella spedizione di un messaggio è necessario contattare il destinatario cui è stata trasmessa per errore la comunicazione chiedendone l'eliminazione del messaggio compresi gli allegati.
Deve essere prestata la massima attenzione nell'aprire allegati di posta elettronica "ambigui" (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati aziendali).
La casella di posta deve essere mantenuta in ordine, conservando le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni o indicazioni operative provenienti da soggetti esterni, e cancellando documenti inutili e soprattutto allegati ingombranti. Il cestino della casella (posta eliminata) deve essere svuotato regolarmente.
E' possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi della casella di posta elettronica certificata amministrazione@pec.aspvenzone.it .
Per la trasmissione di file all'interno dell'Azienda è possibile utilizzare la posta elettronica, evitando di richiedere la ricevuta di lettura per non duplicare le trasmissioni e prestando attenzione alla dimensione degli allegati. Se di dimensioni consistenti si consiglia di utilizzare le cartelle presenti sul server, notificando a mezzo e-mail al destinatario la disponibilità del file stesso.
E' obbligatorio controllare con il software antivirus i files allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

In caso di assenza programmata del lavoratore, il medesimo dovrà attivare un messaggio automatico di risposta alle e-mail ricevute che indichi a quale altro servizio/soggetto inviare messaggi.
Nel caso invece di lunghe assenze non programmate (ad es. per malattia/infortunio), l'Azienda, se necessiti per improrogabili necessità legate all'attività lavorativa di conoscere il contenuto dei messaggi di posta elettronica della casella di servizio dell'utente assente procederà – per il tramite dell'Amministratore di sistema – a richiedere una delega di accesso alla casella di servizio a favore del Responsabile superiore. Di tale attività sarà redatto apposito verbale ed informato l'utente interessato alla prima occasione utile.
In caso di interruzione del rapporto di lavoro con il dipendente (utente), l'indirizzo di posta elettronica personale verrà disabilitato entro un periodo massimo di 20 giorni da quella data.

PARTE SESTA
TRATTAMENTO DI DATI SU DOCUMENTAZIONE CARTACEA

Articolo 35
Archivi cartacei e riproduzione di copie cartacee

Parte del patrimonio informativo dell'Azienda è tuttora presente su supporto cartaceo.
Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro e possibilmente chiuso a chiave. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o anche ad interni non autorizzati al trattamento.
In caso di trattamento di dati personali, tutta la documentazione cartacea deve essere conservata in armadi o cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro o dall'ambulatorio.
L'accesso a tutti i locali aziendali contenenti archivi cartacei deve essere consentito solo a personale preventivamente autorizzato dall'Azienda.
Al momento dello smaltimento, i documenti riservati o contenenti informazioni riservate e/o sensibili e/o categorie particolari di dati personali devono essere distrutti e, ove presenti, triturati nei distruggi documenti appositi.

Articolo 36
Conservazione e archiviazione dei dati sanitari cartacei

Durante il periodo di degenza dei pazienti e degli ospiti, le cartelle e gli altri documenti non devono mai restare incustoditi, neppure all'interno delle sale di medici e infermieri se queste sono accessibili a terzi. Il personale sanitario deve aver cura di riporli tempestivamente negli appositi carrelli o negli armadi presenti all'interno degli ambulatori e di chiudere a chiave i predetti archivi ogniqualvolta vi sia il rischio che il carrello o la sala possano non essere continuativamente presidiati.
La movimentazione delle cartelle sanitarie complete, dal nucleo di degenza verso l'Archivio Sanitario, deve avvenire sempre in fascicoli o faldoni chiusi dai quali non sia desumibile esteriormente alcun dato personale o sanitario. Nei vari tragitti le cartelle non devono mai restare incustodite.
L'accesso all'Archivio sanitario deve avvenire da parte di personale autorizzato e tali locali non devono mai restare incustoditi ed accessibili a terzi nemmeno per brevissimi periodi.
La consegna di referti ambulatoriali esterni che devono essere archiviati in cartella deve avvenire sempre in busta chiusa o utilizzando un contenitore che garantisca che i dati sanitari ivi presenti non siano accessibili a soggetti terzi o comunque non autorizzati, compreso l'operatore che li trasporta.
Le persone autorizzate che provvedono alla duplicazione di documenti contenenti dati sanitari con stampanti, fotocopiatrici o altre apparecchiature, in caso di copia erronea, non correttamente leggibile o comunque non più necessaria sono tenuti a distruggere il documento esclusivamente mediante apposita macchina "distruggi documenti" che garantisca la non leggibilità o ricostruibilità del documento originario.
La consegna della copia della cartella deve avvenire solo una volta accertata l'identità del soggetto richiedente, che deve coincidere con paziente interessato o un soggetto che lo assista e che sia munito dei necessari poteri di rappresentanza (genitori, amministratori di sostegno, tutori) o di apposita delega accompagnata da copia fotostatica del documento d'identità del delegante e del delegato.

PARTE SETTIMA
CONTROLLI, AGGIORNAMENTI E REGIME SANZIONATORIO

Articolo 37
Valutazione d'impatto sulla protezione dei dati

Il Titolare del trattamento effettua, prima di procedere al trattamento medesimo, una valutazione dell'impatto dei trattamenti (art. 35 GDPR) avvalendosi e consultandosi, qualora necessario, con il proprio RDP.
La valutazione è necessaria in particolare nei casi in cui un certo tipo di trattamento, specie quando prevede l'uso di nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche.
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.

La Direzione generale – congiuntamente al RDP - nell'ambito delle attività connesse con il sistema di pianificazione e controllo verifica almeno una volta all'anno l'efficacia e l'efficienza del Sistema, in modo di assicurare l'introduzione di tutte le migliorie necessarie allo stesso e di favorire l'attivazione di un processo di aggiornamento continuo.
Tale valutazione, quando 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'Azienda, prima di procedere al trattamento, consulta il Garante.
L'Azienda, inoltre, attiva tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche individuate dal 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 38
Controlli effettuati dal titolare del trattamento

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali delle Persona Autorizzata e del presente Regolamento.
In caso di anomalie, l'Azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.
In tali casi, il controllo si concluderà con un avviso al Responsabile dell'Area aziendale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'Azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.
In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

Articolo 39
Violazione dei dati personali

La violazione della sicurezza dei dati personali (data breach) corrisponde ad un evento accidentale o illecito che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Tale violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Nel caso in cui la persona autorizzata al trattamento e/o il Responsabile venga a conoscenza di una delle seguenti violazioni:

- accesso o acquisizione dei dati da parte di terzi non autorizzati;
- furto o perdita di dispositivi informatici contenenti dati personali;
- deliberata alterazione di dati personali;
- impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- perdita o distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- divulgazione non autorizzata dei dati personali;

deve provvedere ad informare senza ritardo il Titolare, affinché questi provveda a notificare la violazione all'autorità di controllo competente, con le modalità previste dall'articolo 33 del GDPR.

Articolo 40
Responsabilità e sanzioni

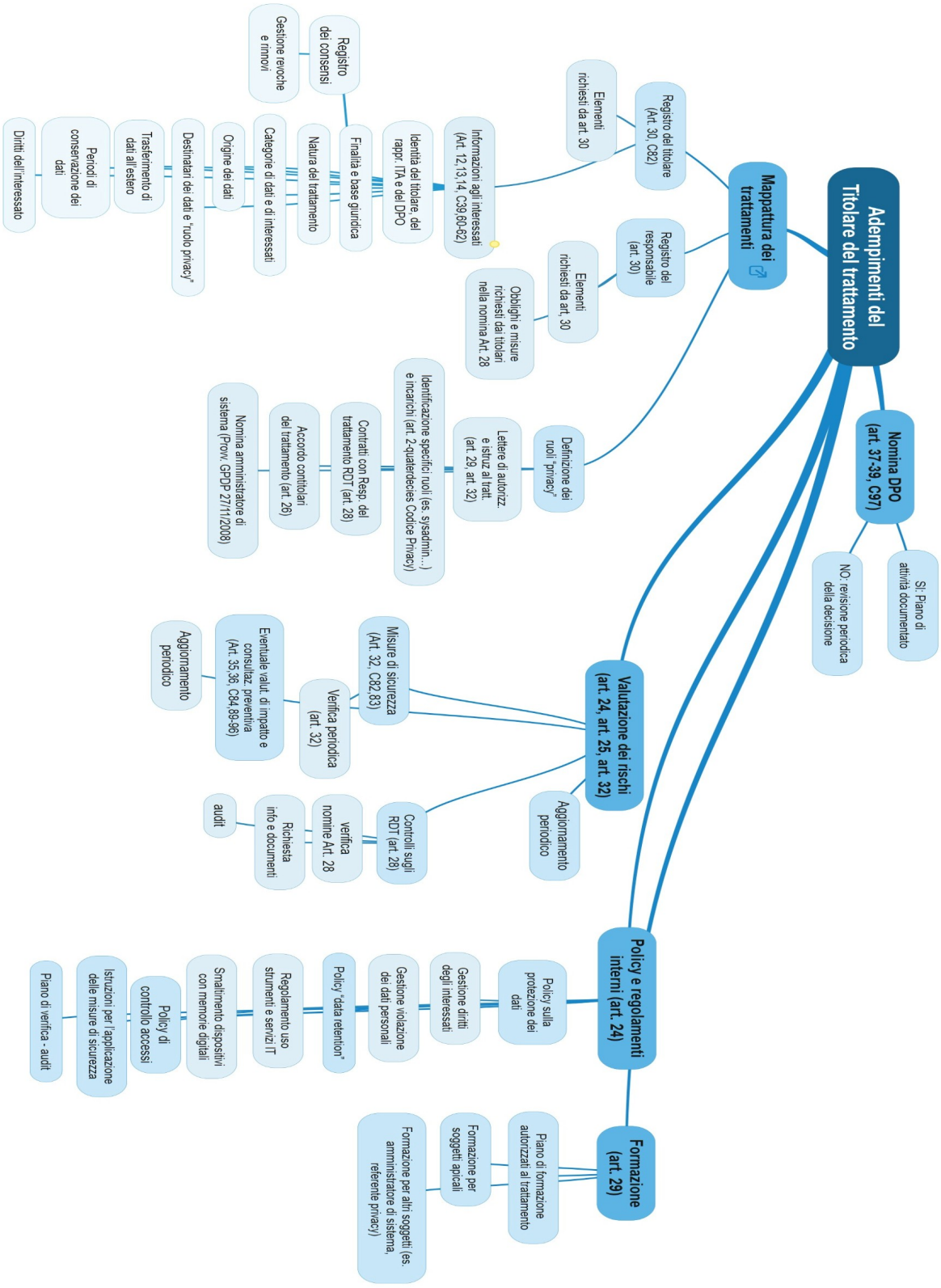
Tutti i soggetti che trattano dati in forza della presente regolamentazione sono tenuti ad adottare comportamenti puntualmente conformi alla normativa vigente, al fine di non esporre l'Azienda e loro stessi a responsabilità nei confronti di terzi ed a rischi sanzionatori.
Essi sono responsabili del corretto trattamento dei dati anche attraverso il corretto utilizzo degli strumenti informatici, dei servizi Internet e posta elettronica. Rispondono pertanto in sede disciplinare, amministrativa, civile e penale per i propri comportamenti contrari alle prescrizioni del GDPR e del presente sistema di regole e dei danni cagionati al patrimonio ed alla reputazione aziendale.
I succitati soggetti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nella presente regolamentazione il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro nel tempo vigente, le azioni civili e penali stabilite dalle leggi vigenti;
- per i collaboratori esterni e i fornitori assegnatari di responsabilità di trattamento dati, oltre che le sanzioni previste dal contratto, le azioni civili e penali stabilite dalle leggi nel tempo vigenti.

Articolo 41
Rinvio

Per tutto quanto non espressamente disciplinato dal presente Regolamento, si applicano le disposizioni previste dal D.Lgs 196 del 30.06.2003, i provvedimenti specifici del Garante per la protezione dei dati personali, nonché le disposizioni del Regolamento Europeo 679/2016.

Allegato 1 – Adempimenti del Titolare del Trattamento



Allegato 2 – Il Registro delle attività di trattamento

Contenuto

Sezione generale:

- Nome e dati di contatto del Titolare del trattamento;
- Nome e dati di contatto del Responsabile della Protezione dei Dati;
- Nome e dati di contatto dei Contitolari del trattamento;

Sezione trattamenti:

- Numero progressivo del trattamento;
- Tipologia di trattamento (breve descrizione del trattamento);
- Ruoli aziendali autorizzati ai singoli trattamenti: Delegati, categorie di autorizzati/incaricati al trattamento e Responsabili del trattamento;
- Tipologia di dati trattati;
- Finalità di trattamento e base giuridica che legittima il trattamento;
- Descrizione delle categorie di interessati;
- Descrizione delle categorie di dati personali e/ particolari e/o relativi a reati e condanne;
- Destinatari o categorie di destinatari a cui i dati sono/saranno comunicati (sia interni che esterni all'organizzazione e compresi i destinatari di paesi terzi od organizzazioni internazionali);
- Se esistono trasferimenti di dati verso paesi terzi o organizzazioni internazionali, indicare quali sono i paesi o le organizzazioni e, se del caso, la documentazione delle "garanzie adeguate" ai sensi del secondo comma dell'art. 46 del GDPR;
- Metodo di conservazione:
  - Cartaceo, indicare i luoghi di conservazione;
  - Digitale, indicare i principali software/database utilizzati per il trattamento ed il luogo di conservazione archivi elettronici, compresi i salvataggi di sicurezza;
- Termini ultimi previsti per la conservazione e successiva cancellazione delle diverse categorie di dati;
- Misure di sicurezza generali, tecniche ed organizzative ed eventuali misure di sicurezza specifiche, adottate per proteggere i dati personali oggetto di trattamento;
- Consenso, indicare se è previsto o non necessario;
- Responsabili del trattamento e durata del contratto;
- Informativa in uso (denominazione e versione);
- Data e versione dell'eventuale DPIA (valutazione di impatto).

Allegato 3 – Le Informative sul trattamento dei dati personali

Contenuto

- identità e dati di contatto del Titolare del trattamento e del suo rappresentante;
- identità e dati di contatto del Responsabile della Protezione dei Dati;
- finalità di trattamento e base giuridica che legittima il trattamento; se la base giuridica è quella del legittimo interesse, specificare qual è il legittimo interesse perseguito dal titolare del trattamento o da terzi;
- natura e modalità del trattamento;
- i destinatari o le categorie di destinatari dei dati e l'ambito di diffusione dei dati medesimi le modalità di trattamento dei dati personali;
- obbligatorietà o meno del conferimento dei dati. Se il conferimento dei dati discende da un obbligo legale o contrattuale od è un requisito necessario a concludere un contratto, l'interessato deve essere informato su tale obbligo e sulle conseguenze della mancata comunicazione dei dati stessi;
- l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e quali sono gli strumenti a garanzia del trasferimento;
- il periodo di conservazione dei dati o criteri seguiti per stabilire tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- 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 revocare il consenso se questo è base giuridica del trattamento;
- il diritto di presentare reclamo all'autorità di controllo (Garante per la protezione dei dati personali);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato