Azienda di Servizi alla Persona
"GOLGI – REDAELLI"

SISTEMA DI GESTIONE DELLA PRIVACY - MODELLO ORGANIZZATIVO DI PROTEZIONE DEI DATI

(REGOLAMENTO UE 2016/679 D. Lgs.196/2003 smi -
protezione delle persone fisiche con riguardo al trattamento dei dati personali)

approvato con Determinazione del Direttore Generale n. 293 del 02.11.2026

1 – OGGETTO E SCOPO **3**
2 - RIFERIMENTI NORMATIVI **3**
3 – DEFINIZIONI **4**
4 – PRINCIPI E LICEITA' DEL TRATTAMENTO **5**
5 - CONTESTO AZIENDALE **8**
6 – RESPONSABILITA' CONNESSE AL TRATTAMENTO DEI DATI **8**
7 – PRINCIPI DI ANALISI DEL RISCHIO, MISURE DI SICUREZZA E CAUTELE **10**
A - TRATTAMENTO EFFETTUATO CON STRUMENTI ELETTRONICI **11**
B - TRATTAMENTO EFFETTUATO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI **14**
C - TRATTAMENTO EFFETTUATO NELL'ESERCIZIO DELLA PROFESSIONE SANITARIA **16**
D - TRATTAMENTO EFFETTUATO NELL'AMBITO DELLA FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI - TRATTAMENTO DI DATI MEDIANTE SISTEMA DOCUMENTALE ELETTRONICO **17**
E - TRATTAMENTO EFFETTUATO NELL'AMBITO DI PRESTAZIONE LAVORATIVA IN SMARTWORKING **17**
F - TRATTAMENTO EFFETTUATO NELL'AMBITO DEL WHISTLEBLOWING **19**
G - TRATTAMENTO EFFETTUATO NELL'AMBITO DELLA POSTA ELETTRONICA AZIENDALE **19**
H - TRATTAMENTO EFFETTUATO NELL'AMBITO DEL SITO WEB ISTITUZIONALE E DEI SOCIAL MEDIA AZIENDALI **20**
I - TRATTAMENTO DI DATI GIUDIZIARI **20**
L - TRATTAMENTO DI DATI IN AMBITO URP **21**
8 - DOCUMENTI DI PRIVACY COMPLIANCE **21**
9 - INFORMAZIONE/FORMAZIONE DEGLI INCARICATI AL TRATTAMENTO **22**
10 - DIRITTO ALLA PROTEZIONE DEI DATI **22**
11 - DPIA – VALUTAZIONE D'IMPATTO **25**
12 - DATA BREACH - VIOLAZIONE DELLA SICUREZZA DEI DATI **26**
13 - MONITORAGGIO E MIGLIORAMENTO DEL SISTEMA **28**

1 – OGGETTO E SCOPO

Il Titolare del trattamento è chiamato a mettere in atto misure tecniche e organizzative adeguate non solo a garantire che il trattamento sia effettuato in conformità alle disposizioni del Regolamento, ma altresì a consentire allo stesso Titolare di dimostrare tale conformità.
Il Sistema di Gestione della Privacy è il modello di gestione, organizzazione e controllo che governa il trattamento in sicurezza dei dati personali ed il rispetto dei principi e delle regole delle normative di riferimento. Per sistema di gestione privacy si intendono la struttura organizzativa, le responsabilità, i documenti, le procedure, i registri, le misure di sicurezza e le risorse messe in atto dall'organizzazione per pianificare, implementare, mantenere e migliorare un sistema di gestione e controllo.

Attraverso l'adozione del Sistema di Gestione, che prevede gli elementi relativi alla organizzazione della sicurezza dei dati e strategie, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dall'ente, l'Azienda intende quindi:
- stabilire politiche e processi atti a conseguire obiettivi di protezione e sicurezza dei dati nel rispetto della normativa in materia, per la salvaguardia dei diritti degli interessati;
- garantire l'osservanza dei principi e delle disposizioni del Regolamento UE e della normativa nazionale di adeguamento attraverso la progressiva implementazione di un sistema strutturato ed organico di procedure e di attività di controllo (ex ante ed ex post) volto a prevenire e/o presidiare eventuali rischi privacy;
- governare in tal modo ogni aspetto dei processi legati al trattamento di dati personali in conformità alla disciplina applicabile;
- creare al proprio interno una cultura della prevenzione del rischio privacy e del controllo dei dati personali trattati nell'ambito del raggiungimento degli obiettivi aziendali, anche attraverso l'implementazione di un sistema di monitoraggio costante dell'attività aziendale che sia in grado di prevenire la commissione di illeciti in materia di privacy e/o di scongiurare la eventuale reiterazione di condotte inosservanti della normativa di settore;
- affermare e diffondere una cultura improntata alla legalità, con espressa riprovazione di qualsivoglia comportamento contrario al GDPR, alla normativa nazionale in materia di protezione dei dati personali e al presente Sistema di Gestione della Privacy;
- introdurre un processo di miglioramento continuo per assicurare la *compliance* alla disciplina di settore.
A tal fine, il presente documento, redatto secondo criteri di sostenibilità da parte dei soggetti chiamati ad applicarlo, enuclea i principi comportamentali e indica le misure necessarie per assicurare che i processi aziendali che implichino un trattamento di dati personali siano gestiti in modo tale da intercettare e tempestivamente governare eventuali situazioni di rischio per la *privacy* degli interessati e, in ogni caso, garantire il puntuale e costante rispetto della disciplina europea e nazionale di riferimento.

Allo scopo, nel presente documento vengono riportate, tra le altre, informazioni riguardo a:
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati
- l'analisi dei rischi cui sono soggetti i dati
- le principali misure utili a garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità, il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

Il documento è parte integrante della politica di privacy e di sicurezza delle informazioni dell'ASP Golgi-Redaelli, insieme alle procedure, istruzioni, lettere di incarico e a tutti gli altri documenti aziendali che recano indicazioni in materia di trattamento dei dati personali. Per l'applicazione generale della normativa in materia di protezione dei dati personali l'Azienda di Servizi alla Persona può altresì dotarsi di ulteriori disposizioni interne, anche a carattere procedurale o regolamentare, alle quali si rimanda per quanto non esplicitato in questo atto.

Con l'adozione di questo documento s'intende, tra le altre cose, richiamare tutte le risorse operanti all'interno dell'Azienda al rispetto della normativa sulla sicurezza dei dati personali.
Periodicamente, il documento viene aggiornato in relazione alla evoluzione della disciplina ovvero di modifiche gestionali e/o organizzative che impattino su di esso.

2 - RIFERIMENTI NORMATIVI

Per la stesura del presente documento, nonché in generale del sistema di protezione dei dati vigente in Azienda (comprensivo del Registro delle Attività di Trattamento) si tiene conto di:

- 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, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Direttive e Linee guida del Parlamento Europeo in materia
- Autorizzazioni generali, provvedimenti, codici di condotta, regole deontologiche specifiche e indicazioni diverse del Garante della Privacy vigenti nel tempo, cui si fa espresso richiamo.

Vengono fatti salvi gli ulteriori aggiornamenti e disposizioni normative, regolamentari e determinazioni delle Autorità preposte eventualmente sopravvenute, da intendersi qui parimenti citati.
Le attività di protezione della privacy e di tutela dei dati personali vengono poste in essere nei più generali ambiti della normativa in materia di Pubblica Amministrazione applicabili all'Azienda e della legislazione specifica che regola le Aziende di Servizi alla Persona, con particolare riferimento alle disposizioni emanate al proposito dalla Regione Lombardia.

3 – DEFINIZIONI

Secondo le previsioni di cui al Regolamento Europeo 2016/679, come recepite in sede nazionale (anche con provvedimenti diversi del Garante della Privacy), si intende:

a) per *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; sono, quindi, *dati personali* le informazioni che identificano o rendono identificabile – direttamente o indirettamente – una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.
   Rilevano, particolarmente:
   - Dati che permettono l'identificazione diretta, quali: dati anagrafici, immagini etc.
   - Dati che permettono l'identificazione indiretta, quali: codice fiscale, indirizzo IP, numero di targa etc.
   - Dati rientranti in particolari categorie (dati sensibili), che rivelano l'origine razziale o etnica, le convinzioni religiose o filosofiche, le opinioni politiche, l'appartenenza sindacale, gli orientamenti sessuali etc, nonché
     dati genetici: il dato personale relativo 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: il dato personale ottenuto da un trattamento tecnico specifico e relativo 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: il dato personale attinente 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;
   - Dati relativi a condanne penali e reati (dati giudiziari), che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale, o la qualità di imputato o indagato, o l'assoggettamento a correlate misure di sicurezza;
   - Dati riferiti alle comunicazioni elettroniche (mail, internet, telefono) o che consentono la geolocalizzazione fornendo informazioni su luoghi frequentati e sugli spostamenti.

b) per *trattamento del dato*: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, utilizzo, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione, distruzione,

c) per *Titolare del trattamento dei dati*: persona fisica o giuridica, autorità pubblica, ente pubblico o privato etc. che adotta le decisioni sugli scopi e sulle modalità del trattamento

d) per *Responsabile del trattamento dei dati*: persona fisica o giuridica esterna all'Ente alla quale il titolare chieda di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati. E' possibile anche che il medesimo, secondo determinate condizioni, designi un sub-responsabile

e) per *AUTORIZZATO/Incaricato del trattamento dei dati*: soggetto individuato per la gestione operativa delle attività di trattamento

f) per *Amministratore di sistema*: soggetto individuato dal Titolare del Trattamento per la gestione e la manutenzione di un impianto di elaborazione o di sue componenti, o figura equiparabile dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi

g) per *Responsabile della Protezione dei Dati*: un soggetto in possesso di adeguata professionalità che svolge le attività di competenza specifica previste dal DGPR

h) per *Interessato*: la persona fisica alla quale si riferiscono i dati personali

4 – PRINCIPI E LICEITA' DEL TRATTAMENTO

Principi generali del trattamento di dati personali
Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679:
- liceità, correttezza e trasparenza del trattamento nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati, pertinenti, non eccedenti, indispensabili e limitati a quanto necessario rispetto alle finalità del trattamento perseguite nei singoli casi;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Liceità del trattamento di dati personali
Ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono:
- consenso,
- adempimento obblighi contrattuali,
- interessi vitali della persona interessata o di terzi,
- obblighi di legge cui è soggetto il titolare,
- interesse pubblico o esercizio di pubblici poteri,
- interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Il trattamento di **"categorie particolari di dati personali"** (dati 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, ved. art.3, lett. a, terzo punto), è vietato a meno che il Titolare dei Trattamenti dell'ASP possa dimostrare di soddisfare almeno una delle seguenti condizioni:

- l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per uno dei seguenti scopi:
  - 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;
  - 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;
  - per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
  - per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
  - 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;
  - per motivi di interesse pubblico nel settore della sanità pubblica (se tali dati sono trattati sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza);
  - per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

I dati trattati sono essenziali per lo svolgimento delle attività istituzionali, quando le finalità di interesse pubblico non possono essere adempiute mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Questi dati non possono essere diffusi.

(Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale).

Consenso

Quando il trattamento si fonda sul consenso dell'interessato, il Titolare deve sempre essere in grado di dimostrare che l'interessato ha prestato il proprio consenso, che è valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali;
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse.

La richiesta di consenso deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato per esempio all'interno di modulistica.
Quando il trattamento riguarda le "categorie particolari di dati personali" il consenso deve essere "esplicito"; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione).
Non è comunque ammesso il consenso tacito o presunto (per esempio, presentando caselle già spuntate su un modulo).
Il consenso deve essere sempre revocabile.

Interesse vitale di un terzo

Si può invocare tale base giuridica per il trattamento di dati personali solo se nessuna delle altre condizioni di liceità può trovare applicazione.

Interesse legittimo prevalente di un titolare o di un terzo

Il ricorso a questa base giuridica per il trattamento di dati personali presuppone che il titolare stesso effettui un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato.
L'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.

L'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.
Il legittimo interesse non può essere invocato isolatamente quale base giuridica per il trattamento delle "categorie particolari di dati personali".

Motivi di interesse pubblico rilevante sulla base del diritto italiano (D.Lgs.196/2003 smi)
E' rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle materie individuate all'art. 2-sexies del d. Lgs., tra le quali per l'ASP Golgi-Redaelli rilevano o potrebbero rilevare in particolare:
- accesso a documenti amministrativi e accesso civico
- tenuta di registri pubblici relativi a beni immobili o mobili
- esercizio del mandato degli organi rappresentativi, ivi compresa la sospensione o lo scioglimento, nonché l'accertamento di cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche
- concessione, liquidazione, modifica, e revoca di benefici, agevolazioni, elargizioni, altri emolumenti e abilitazioni
- accertamento di requisiti di onorabilità e di professionalità per le nomine ad uffici e cariche direttive di persone giuridiche ed imprese
- concessione di patrocini
- adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali
- rapporti con gli enti del terzo settore
- attività di tutela in sede amministrativa o giudiziaria
- rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose
- attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti ed incapaci
- attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi comprese le trasfusioni di sangue umano
- compiti del SSN e dei soggetti operanti in ambito sanitario
- compiti di igiene e sicurezza sui luoghi di lavoro
- salvaguardia della vita e dell'incolumità fisica
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, compresa instaurazione e gestione dei rapporti con soggetti accreditati con il SSN
- farmacovigilanza
- istruzione e formazione in ambito professionale
- archiviazione o ricerca storica concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti nell'archivio storico
- ricerca scientifica
- instaurazione, gestione, estinzione di qualsiasi rapporto di lavoro, materia sindacale, collocamento, previdenza e assistenza, pari opportunità, obblighi retributivi fiscali o contabili, igiene e sicurezza del lavoro o della popolazione

Il trattamento svolto per l'adempimento di **un compito svolto nel pubblico interesse** o **per l'esercizio di pubblici poteri** non può arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-bis del D. Lgs. 196/2003. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis del D. Lgs. 196/2003.

Trattamento di dati relativi a condanne penali e reati
Al ricorrere di una delle fattispecie seguenti (trattamento in base a consenso dell'interessato, per l'esecuzione di un contratto o di misure precontrattuali su richiesta dell'interessato, in base a obbligo di legge, per la salvaguardia di interessi vitali dell'interessato, per lo svolgimento di un compito di interesse pubblico, per il perseguimento di un legittimo interesse del titolare), è consentito se autorizzato da leggi o regolamenti riguardanti in particolare, per l'ASP Golgi-Redaelli:
- adempimento di obblighi e esercizio di diritti in materia di diritto del lavoro o nell'ambito di rapporti di lavoro

- accertamento e verifica di requisiti di idoneità morale, onorabilità, requisiti soggettivi, presupposti interdittivi
- accertamento di responsabilità per sinistri e eventi attinenti alla vita umana
- accertamento, esercizio, difesa di un diritto in sede giudiziaria
- esercizio del diritto di accesso a dati e documenti amministrativi
- esecuzione di investigazioni, ricerche, raccolta di informazioni
- adempimenti di obblighi in materia di antimafia e altre gravi forme di pericolosità sociale, anche per la produzione di documentazione per partecipare a gare d'appalto

5 - CONTESTO AZIENDALE

L'Azienda di Servizi alla Persona Golgi-Redaelli è un Ente Pubblico non Economico senza scopo di lucro, ai sensi della Legge Regione Lombardia del 13 febbraio 2003 n. 1 e smi. E' dotata di autonomia organizzativa, gestionale, contabile.
La *mission istituzionale* dell'Azienda è fornire prestazioni sanitarie, assistenziali e di recupero funzionale e sociale a una popolazione prevalentemente anziana, non autosufficiente e a rischio di perdita di autonomia sia presso le tre strutture operative (Istituti geriatrici) site nei Comuni di Milano, Vimodrone e Abbiategrasso, sia al domicilio; l'Azienda eroga prestazioni in *regime residenziale (Residenze Sanitarie Assistenziali/RSA - Cure Intermedie - Nuclei Alzheimer - Hospice - Stati vegetativi permanenti), *semiresidenziale (Servizi Riabilitativi di Ospedale Diurno (DH), di Ciclo Diurno Continuo (CDC) e Centro Diurno Integrato (CDI), RSA Aperta), *ambulatoriale (specialistiche, in diverse branche: analisi chimico - cliniche, geriatria, cardiologia, radiologia, riabilitazione…); a soggetti in età evolutiva per riabilitazione neuropsicologica e *counseling* educativo-abilitativo per minori affetti da autismo), *territoriali, di assistenza domiciliare.
L'Azienda inoltre provvede alla gestione di proprio patrimonio immobiliare urbano e rurale, alla conservazione, tutela, integrazione, valorizzazione e divulgazione del patrimonio di interesse storico-artistico-culturale, ed esplica attività di prevenzione, studio e ricerca anche di carattere epidemiologico, clinico e sociale.
L'ASP Golgi-Redaelli attiva altresì iniziative al fine precipuo di far conoscere i propri servizi e promuovere attività ed eventi connessi agli stessi, gestisce e sviluppa un sistema di relazioni per fidelizzare il rapporto con l'utenza e con i soggetti che abitualmente interagiscono con l'Azienda, innova ed ottimizza i servizi avvalendosi di strumenti di customer satisfaction.
L'ASP si avvale complessivamente di circa 1.200 dipendenti, fra cui personale amministrativo, tecnico, medico e paramedico e assistenziale.
Il Direttore Generale è il Direttore e Legale Rappresentante dell'Azienda e, tra le altre cose, per il tramite della struttura organizzativa aziendale, come definita nel tempo, traduce in atto le politiche deliberate dal Consiglio.
Per l'assetto organizzativo, l'attribuzione degli incarichi di struttura ed il relativo funzionigramma si rimanda alle sezioni di riferimento del sito web aziendale.

6 – RESPONSABILITA' CONNESSE AL TRATTAMENTO DEI DATI

- *"Titolare del trattamento dei dati"* è l'Azienda di Servizi alla Persona "Golgi-Redaelli", legalmente rappresentata dal Direttore Generale.
  (*"Titolare del trattamento dei dati"* limitatamente alle finalità di medicina del lavoro è il medico competente aziendale individuato e nominato dal Datore di Lavoro)

- *"Responsabile della protezione dei dati"* è un dirigente di ruolo dell'Azienda in possesso dei requisiti di legge, e risponde alla mail privacy@golgiredaelli.it.
  Si occupa principalmente di:
  *sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità; *collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA); *informare e sensibilizzare il titolare o i responsabili del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati; *cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento; *supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

- *"Responsabili del trattamento dei dati"* possono essere soggetti esterni o terzi all'Azienda (qualora gestori di banche dati originate dal rapporto contrattuale instaurato con l'Azienda), e tra gli altri:

- le Aziende che concorrono alla realizzazione del SISS, come di volta in volta segnalate con specifiche comunicazioni dalla Regione Lombardia relativamente ai dati trattati nell'ambito del sistema in questione;
- fornitori diversi e altri soggetti, nell'ambito di servizi o prestazioni da questi ultimi eseguiti in favore dell'Azienda;
- soggetti con cui intercorrono convenzioni, protocolli di intesa e accordi diversi.

Si occupano principalmente di:
*trattare dati personali per conto del titolare del trattamento e su istruzione di questi, mettendo in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato; *garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; *mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alle vigenti normative, *su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento.

Rapporti con i Responsabili esterni del Trattamento
La nomina a Responsabile esterno del Trattamento va adeguatamente contrattualizzata, come da apposite indicazioni aziendali vigenti, a cura del Dirigente competente alla redazione degli accordi con il soggetto terzo. Ai fini dell'efficacia delle stesse, le istruzioni devono essere personalizzate, almeno per tipologia di fornitore/soggetto da incaricare e di attività svolta. La corretta applicazione delle istruzioni e dei requisiti di sicurezza richiesti alle terze parti che si configurano come Responsabili Esterni del Trattamento vanno verificate da parte del Dirigente competente per materia o, nel caso di forniture o servizi esternalizzati, da parte del dirigente responsabile dell'esecuzione del contratto.

- *"Autorizzati/Incaricati del trattamento dei dati":* ciascun dipendente formalmente assegnato ad una struttura organizzativa o preposto allo svolgimento di un'attività che prevede il trattamento dei dati (compresi dirigenti, funzionari e titolari di incarichi di coordinamento/organizzazione) riveste automaticamente la qualifica di "autorizzato/incaricato del trattamento" per i dati di competenza in relazione alle mansioni effettivamente svolte, all'ufficio, al servizio, alla sede di assegnazione – senza necessità di ulteriore individuazione nominativa - ed è autorizzato a compiere le relative operazioni attenendosi alle istruzioni impartite, come individuate anche nel Registro delle Attività di Trattamento per ogni trattamento specifico; i rispettivi Dirigenti curano la definizione dei compiti degli stessi in base alla organizzazione interna di settore, e forniscono le istruzioni del caso anche in materia di gestione in sicurezza delle banche dati e degli archivi correnti di riferimento di pertinenza.
  Nel caso di eccessiva onerosità delle attività utili a fornire le informazioni singolarmente ad ogni incaricato del trattamento, ad esempio quando lo stesso faccia riferimento ad una categoria omogenea di persone (medici, infermieri, personale dipendente di reparto coinvolto nel trattamento di dati degli ospiti,.....) è possibile fornire le istruzioni del caso, che dovranno essere opportunamente diffuse e divulgate agli interessati, via mail o anche mediante esposizione in luogo visibile ed accessibile alla totalità degli incaricati.
  In mancanza della documentata preposizione delle persone fisiche alle unità organizzative, il Dirigente autorizzato al trattamento dei dati di assegnazione provvede a formalizzare gli incarichi in tal senso avuto riguardo alle competenze degli Uffici diretti.

  Gli incaricati del trattamento si occupano, tra le altre cose, di:
  *trattare i dati secondo le modalità in uso in Azienda; *trattare i dati in modo lecito e secondo correttezza; *effettuare le sole operazioni di trattamento necessarie allo svolgimento della propria mansione; *attenersi alle istruzioni impartite; *applicare le misure di sicurezza adottate dall'Azienda al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati personali; *prevenire e/o evitare la comunicazione o diffusione illecita dei dati; *astenersi dall'adozione di autonome decisioni in merito alle finalità o modalità di trattamento dei dati; *informare tempestivamente il proprio Responsabile di ogni questione rilevante in merito al trattamento dei dati.

- *"Amministratore di Sistema"*, individuato per l'Azienda nel Funzionario preposto al Servizio Sistemi Informativi
  Per le attribuzioni del medesimo, si veda oltre, al punto 7-A.

Banche dati ed archivi

L'Azienda implementa **banche dati ed archivi**, informatizzati o meno, in taluni casi di carattere trasversale e su cui intervengono e alla cui gestione concorrono - ciascuna per la parte necessaria per lo svolgimento delle attività di rispettiva competenza - diverse strutture operative. Ne sono responsabili, ciascuno per la parte di competenza in relazione ai trattamenti effettuati, i Dirigenti ed il personale assegnati alle singole strutture.

I dati afferenti alle banche dati ed archivi possono essere conosciuti ed utilizzati anche da strutture aziendali a qualsiasi titolo coinvolte in attività per i quali gli stessi si rendano necessari, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle incombenze di assegnazione.

Al proposito, si evidenzia che il Personale appartenente all'Azienda dovrà sempre:
i. trattare dati solo ed esclusivamente al fine di svolgere le mansioni per le quali è stato appositamente autorizzato, e per nessun motivo, trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative;
ii. operare e trattare dati secondo principi di correttezza, riservatezza, necessità, buona fede e esclusivamente per scopi leciti;
iii. utilizzare gli strumenti informatici hardware e software in dotazione anche temporanea per scopi strettamente aziendali, nel rispetto delle istruzioni fornite e delle norme di legge applicabili e comunque mai contrari all'ordine pubblico, al buon costume e alla morale.
iv. utilizzare le proprie competenze tecnico-informatiche per salvaguardare i beni aziendali da qualunque tipo di software dannoso (malware) o anche potenzialmente nocivo o che metta in pericolo la sicurezza o l'integrità del sistema stesso.
v. segnalare ogni eventuale lacuna o difficoltà dovesse incontrare, in relazione agli obblighi di cui al presente MOP, nell'esecuzione del lavoro.

7 – PRINCIPI DI ANALISI DEL RISCHIO, MISURE DI SICUREZZA E CAUTELE

Viene posto in essere un preliminare e periodico processo di *risk assessment* finalizzato alla valutazione del "rischio *privacy"* – ovverossia dell'eventuale impatto negativo sulle libertà e i diritti degli interessati - connesso alle attività di trattamento di dati personali effettuate, condotto mediante analisi dei dati personali trattati e degli strumenti organizzativi, di gestione e di controllo volti a verificare la rispondenza dei principi comportamentali, delle procedure e/o delle prassi organizzative in essere ai principi, regole e finalità dettati dal Regolamento UE e, ove necessario, ad integrare le misure di sicurezza organizzative e tecniche per assicurarne l'adeguatezza, tenuto conto del contesto di riferimento. Il rischio viene calcolato mediante i parametri di probabilità, impatto e vulnerabilità e l'analisi è centrata su

- rischi derivanti da contenuto intrinseco del trattamento
- rischi derivanti da possibili violazioni di sicurezza

in relazione ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

A livello aziendale vengono individuati i seguenti **macrofattori di rischio** relativi ai dati trattati:

- rischio di danneggiamento, modifica, distruzione o perdita, correlati ad eventi relativi al contesto in cui si opera o relativi agli strumenti
- rischio di accesso non autorizzato, di trattamento non autorizzato, di rivelazione, di modifica, di trattamento non conforme alla finalità della raccolta o illecito, correlato a comportamenti degli operatori

-

Il trattamento dei dati viene effettuato, secondo criteri di integrità e riservatezza, in modo da garantirne l'adeguata sicurezza, compresa la protezione mediante **misure tecniche, organizzative e di sicurezza** - rispetto a trattamenti non autorizzati o illeciti, non consentiti o non conformi alle finalità della raccolta, ovvero alla perdita, distruzione o danno accidentale – di cui al presente ed ai successivi articoli che riguardano l'adozione di idonei e preventivi accorgimenti, in ordine ai rischi rilevati.
In particolare, vengono adottate tra le altre le seguenti principali misure:

- organizzative, quali: istruzioni interne; assegnazione di incarichi; formazione agli addetti; classificazione dei dati; distruzione controllata dei supporti; aggiornamento periodico degli ambiti di trattamento consentiti agli incaricati o alle unità organizzative
- fisiche, quali: vigilanza delle sedi di custodia dei dati; custodia in classificatori o armadi non accessibili; dispositivi antincendio; continuità dell'alimentazione elettrica; verifica della leggibilità dei supporti

- logiche, quali: identificazione dell'incaricato e/o dell'utente; controllo degli accessi a dati e programmi; controlli aggiornati antivirus; monitoraggio continuo delle sessioni di lavoro; controllo dei supporti consegnati in manutenzione

A - TRATTAMENTO EFFETTUATO CON STRUMENTI ELETTRONICI

Le attività condotte in Azienda prevedono l'utilizzo di strumenti elettronici quali elaboratori o personal computer, anche portatili, connessi alla rete aziendale. Grazie alla suddetta interconnessione da ogni postazione di lavoro sono usufruibili (in base ad una opportuna profilazione degli utenti interni) le informazioni presenti sulle banche dati attraverso i software gestionali dedicati alle varie attività.

I server aziendali in cui sono memorizzate le principali basi dati, sono collocati nella sala server principale. Ulteriori server periferici, adibiti principalmente per l'assegnazione degli indirizzi IP, sono collocati in ogni rete locale afferente ad ogni struttura (sede). Su di essi sono inoltre predisposti delle quote disco condivise per consentire marginali attività collaborative.

Il sistema è presidiato a livello centralizzato da un Amministratore di Sistema che – anche avvalendosi dei dipendenti facenti capo al Servizio Sistemi Informativi aziendale – ha il compito di sovrintendere alle risorse del sistema informatico in termini di hardware, sistemi operativi, sistemi per la gestione di basi di dati, applicazioni informatiche (cioè software di base e applicativo) e reti e di consentirne l'utilizzazione, come pure di a garantire, in relazione alle conoscenze informatiche acquisite in base al progresso tecnologico, lo sviluppo delle misure di sicurezza necessarie al fine di: a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati su supporti magnetici e ottici gestiti, nonché delle banche dati e dei locali ove esse sono collocate; b) evitare l'accesso non autorizzato alle banche dati, alla rete e, in generale, ai servizi informatici dell'Azienda; c) prevenire trattamenti di dati non conformi alla legge od ai regolamenti; d) evitare la cessione o la distribuzione dei dati in caso di cessazione del trattamento.
Anche a tal fine l'Azienda – in un'ottica informativa e formativa - può mettere a disposizione degli utenti interni, attraverso piattaforme condivise, indicazioni, documenti, procedure operative di carattere generale e/o riguardo a specifici argomenti in materia.

Rischio	**Misura**	**Possibili ulteriori misure**
danneggiamento, distruzione o perdita del dato	- effettuazione di copie di sicurezza, salvataggio settimanale dei dati, backup centralizzato periodico dei programmi di protezione per elaboratore (semestrale per trattamento di dati sensibili o giudiziari) - effettuazione di backup full dei database dei gestionali giornalieri conservando gli ultimi 7 - back up in cloud su Object Storage - backup quotidiano dei Sistemi Operativi virtuali presenti sull'infrastruttura principale (DATACORE) su NAS appositamente adibito (DR), collocato nella sala server secondaria, e successiva copia di ogni vm sul cloud, con una retention di 5. Per le vm principali è inoltre impostata la CDP (Continuos Data Protection) che consente un'attivazione in tempi brevi del servizio eventualmente coinvolto in un malfunzionamento/errore/danno hardware o software, consentendo il recupero della vm al minuto precedente. Il CDP ha una retention di circa 48 ore. - Servizio MDR (Managed Detection and Response) H24x7x365sulle VM presenti in infrastruttura erogato da un SOC (Security Operations Center) conseguendo un notevole rafforzamento delle politiche di sicurezza	- sistematizzare formazione e informazione in materia

	- effettuazione periodica di restore (dei dati di backup) del database del gestionale principale; - ripristino periodico delle vm conservate sia su NAS locale che su cloud; - dotazione di impianti antincendio - adozione di sistemi di ridondanza sui server - presenza di almeno due alimentatori su ogni server - utilizzo di dischi con RAID e hotspare sui sistemi di produzione - utilizzo di infrastrutture servite da alimentazione privilegiata (gruppo elettrogeno) ed UPS per i sistemi di produzione - adozione di accorgimenti di cybersecurity attraverso la realizzazione di corsi e l'emanazione di indicazioni atte a responsabilizzare gli utenti interni sui rischi connessi all'utilizzo degli strumenti elettronici e sui comportamenti e misure da adottare per limitare/abolire danni correlati	
<u>accesso non autorizzato (ai locali, al sistema ed ai dati)</u>	- i server aziendali sono collocati in locali chiusi a chiave (porte blindate o tradizionali), di norma senza finestre e in taluni casi dotati di telecamera IP con registrazione remota - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate - assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate - adozione di sistema di gestione degli utenti (LDAP – Active Directory) che associa il data base degli stessi con le rispettive autorizzazioni, disponibile centralmente in rete al fine di un eventuale recupero su richiesta dei soggetti autorizzati al trattamento dei dati, che costituisce un sistema di SSO (Single-Sign-On) per gli accessi ai gestionali principali e alle caselle e.mail. - blocco delle PdL in caso di inattività. Regola impostata a livello centrale, senza possibilità di variazione da parte dell'utente. - tutti i PC fissi e mobili e gli elaboratori sono coperti da sistemi di rilevamento e di prevenzione delle intrusioni, firewall di sistema, antivirus, antispyware la cui efficacia è periodicamente verificata ed aggiornata - tutte le PdL sono governate da un sistema centralizzato con funzioni di inventario hardware e software, controllo remoto, software distribution,patch e risk management. - attivazione di switch e access point di rete in cui sono state configurate VLAN - impostazione del controllo degli accessi sugli apparati di rete (gli apparati con management sono protetti con credenziali di accesso) - la protezione perimetrali delle LAN è garantita da Firewall di nuova generazione.	- sistema di tracciabilità degli eventuali accessi di personale non-CED - definizione di istruzioni per l'uso, la custodia e la distruzione dei supporti rimovibili o del contenuto degli stessi, al fine di evitare accessi non autorizzati e trattamenti impropri - apposizione di clausole di sicurezza ai contratti di manutenzione software – ove non già esistenti

trattamento non autorizzato	- ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore - di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; - i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - implementazione di regole centralizzate finalizzate ad aumentare la robustezza delle password - disattivazione dei codici personali nel caso in cui vi sia perdita della qualifica che permette l'accesso all'operatore o di mancato utilizzo superiore ai sei mesi o altro periodo stabilito mediante incrocio delle informazioni provenienti dal gestionale HR con le credenziali di accesso in LDAP	- valutazione delle modalità di utilizzo di tecniche di anonimizzazione, cifratura o codici identificativi o di altre soluzioni che rendano temporaneamente inintelligibili i dati - trasferimento cifrato dei dati sensibili e giudiziari in formato elettronico (già attivo per VPN)
trattamento non conforme alla finalità della raccolta o illecito	- è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.	///

Il Titolare del trattamento dei dati, per il tramite del Dirigente responsabile del Servizio Sistemi Informativi aziendale e con il supporto dell'Amministratore di Sistema provvede a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative di cui sopra, anche mediante l'adozione di apposite procedure, nonché a controllarne a campione il rispetto da parte degli utenti interni.

- utilizzare le proprie credenziali di autenticazione (username e password) in modo diligente, evitando di lasciare aperta e senza il proprio controllo diretto una sessione di lavoro con risorse o applicativi ai quali si è acceduto con tali credenziali, ed impostando se possibile gli applicativi online e offline in modo da prevedere una scadenza della sessione dopo un prolungato periodo di inattività (attivazione screen saver con password) (policy aziendale configurabile sul Domain Controller);
- custodire le proprie credenziali in un luogo sicuro, non facilmente individuabile o poco sorvegliato, ed avvisare tempestivamente il Responsabile del Trattamento in caso di smarrimento o sottrazione;
- modificare la password fornita al primo accesso, e poi ogni 3 mesi (configurata sul Domain Controller);

- adottare password formate da non meno di 8 caratteri alfanumerici, contenenti almeno una lettera maiuscola e un numero, ed in ogni caso diverse dalle ultime utilizzate (configurata sul Domain Controller);
- mantenere segrete le proprie credenziali di autenticazione o quantomeno la password, evitando di rivelarla o di farla utilizzare a terzi;
- non utilizzare le stesse credenziali (password) per l'accesso ai diversi servizi online (es. Posta elettronica dell'Azienda, Facebook, Home banking, Posta elettronica personale, ecc.),
- attivazione del Single sign-on (SSO). Le credenziali di accesso gestire sul Domain Controller sono utilizzabili per l'accesso ai seguenti gestionali: MyCare, IntraIpab, GPI – Angolo del Dipendente, Suite HR, LABANA, SIAV, IrisWeb (dismesso il 31/12/2021) ePersonam (Advenias), Vettore (DoctoLib). Restano da integrare MODULAB (che verrà integrato nei prossimi mesi) ed i servizi Vianova (email, meeting, ecc.) Il requisito di integrazione al Domain Controller aziendale è richiesto per ogni nuova fornitura di software gestionale.
- conservare eventuali supporti magnetici rimovibili utilizzati nel trattamento (es. CD, dischetti, pen drive USB) con i medesimi accorgimenti previsti per i supporti cartacei, provvedendo a cancellarne i dati prima dell'eventuale reimpiego da parte di soggetti non autorizzati;
- curare l'aggiornamento delle risorse informatiche e degli applicativi o, laddove non possibile direttamente, inoltrare ai referenti informatici o al Responsabile del Trattamento le segnalazioni di aggiornamento ricevute;
- non aprire e-mail o allegati dall'incerta o pericolosa provenienza e non installare programmi scaricati da siti non ufficiali o comunque di natura incerta;
- evitare di gestire i dati personali in relazione all'attività istituzionale su piattaforme o servizi online, mediante l'accesso da PC di terzi o dispositivi (es. smartphone) collegati a Internet
- NON asportare dati personali dalla sede di lavoro mediante supporti magnetici, tablet o cellulari, o device similari
- NON utilizzare Google Drive o similari
- NON utilizzare chat personali per il trasferimento o lo scambio di dati personali e/o documenti contenenti dati personali (compresi sensibili, super-sensibili e giudiziari)
- NON utilizzare la casella mail come archivio di dati o documenti.

In caso di utilizzo di strumenti messi a disposizione da soggetti esterni (piattaforme, software gestionali, server esternalizzati, etc.....) la responsabilità di garantire la sicurezza, la tutela e la riservatezza del dato ricade sul fornitore, che è tenuto ad assicurare un prodotto adeguato e rispettoso delle vigenti normative in materia.

B - TRATTAMENTO EFFETTUATO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Tale trattamento prevede che i dati siano conservati in archivi cartacei o su supporti di tipo magnetico e/o ottico.

Rischio	**Misura**
accesso non autorizzato	- la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato; i locali in cui sono conservati tali documenti devono essere chiusi al termine dell'orario di lavoro - i documenti contenenti dati sensibili, se affidati all'incaricato del trattamento, devono da questo essere

	conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio - l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni - i documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro - fare attendere soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, avere cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c. - evitare l'esportazione di dati personali e/o l'installazione degli stessi su attrezzature diverse da quelle messe a disposizione dall'Azienda (ad es. computer di casa)
<u>trattamento non autorizzato</u>	- gli incaricati al trattamento sono autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento - divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate - i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative - il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Azienda avviene in modo da garantirne la riservatezza
<u>trattamento non conforme alla finalità della raccolta o illecito</u>	- i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo - è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi - a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili. - i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti

Oltre a quanto sopra, inoltre, si avrà cura di adottare, tra le altre, le seguenti <u>misure organizzative:</u>

- ❑ restituire gli atti ed i documenti al termine delle operazioni di trattamento o riporli in zone ad accesso controllato;
- ❑ non trasportare fuori del luogo di lavoro atti o documenti contenenti dati personali, salvo espressa autorizzazione del Responsabile del Trattamento;
- ❑ laddove previsto, procedere all'identificazione e registrazione del proprio accesso agli archivi, qualora questo avvenga oltre l'orario di lavoro;
- ❑ custodire diligentemente le chiavi dei locali o degli armadi in cui vengono conservati i dati cartacei, evitando di cederle a terzi e comunicandone tempestivamente lo smarrimento o il furto al proprio referente;
- ❑ prelevare i documenti dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni;
- ❑ richiedere autorizzazione al Responsabile del Trattamento per le operazioni di copia, stampa, trasmissione, consegna a soggetti esterni o non autorizzati, creazione di nuove banche dati o riorganizzazione delle attuali, effettuate con qualunque modalità e verso qualunque supporto, custodendo le copie con le stesse modalità degli originali.

C - TRATTAMENTO EFFETTUATO NELL'ESERCIZIO DELLA PROFESSIONE SANITARIA

Il trattamento in questione, se effettuato con strumentazione informatica o in modo non informatizzato, partecipa dei rischi generali e delle misure di limitazione degli stessi individuate alle precedenti lettere A e B.
Gli adempimenti di privacy coinvolgono anche i **dispositivi medici** (DM o **elettromedicali**) utilizzati in Azienda - con particolare riferimento alle strumentazioni di Radiologia e afferenti al Laboratorio di Analisi - se e in quanto contengano dati personali e dati relativi alla salute dei pazienti, acquisiti dalla *worklist* (ovvero la lista di lavoro delle prestazioni da eseguire sul macchinario) e nel corso della prestazione sanitaria, e siano configurati per inviare tali informazioni ad altri dispositivi, per la refertazione e la conservazione dei dati necessari a fornire una diagnosi e a stabilire il percorso di cura del paziente, in regime ambulatoriale o di ricovero.
In tal caso, fatta salva l'importanza di garantire che l'invio delle informazioni ad altri applicativi dedicati avvenga nella massima sicurezza informatica, attraverso protocolli di rete sicuri e verificando regolarmente che non vi siano potenziali vulnerabilità, occorre che i dati inoltrati non restino immagazzinati anche all'interno dello *storage* del singolo apparecchio, ma vengano cancellati.
Quando, invece, l'elettromedicale non si interfacci o non sia integrato con altri applicativi, a prescindere dalla necessità di procedere a frequenti controlli periodici sulla conservazione in sicurezza dei dati, l'apparecchio dovrà mantenere memorizzate le informazioni relative alla prestazione del paziente fintantochè non si sia provveduto ad una conservazione sostitutiva delle medesime.

Lo sviluppo in Azienda della **Cartella clinica elettronica**, come pure l'approccio ad attività di **Telemedicina**, devono trovare soluzioni tecniche e logico-organizzative rispettose delle esigenze di massima tutela dei dati e dell'utenza, seppure in ambiti e contesti con carattere innovativo a fronte delle consuete modalità operative dell'ASP.

Oltre a quanto sopra, inoltre, con particolare riguardo alle problematiche di tutela della privacy nell'**esercizio della professione sanitaria e delle attività correlate**, si avrà cura di adottare, tra le altre, le seguenti misure organizzative:

- chiamata degli interessati prescindendo dall'individuazione nominativa degli stessi in caso di prenotazione e attesa
- accorgimenti utili al rispetto delle distanze di cortesia
- soluzioni atte a garantire la riservatezza dei colloqui
- cautele volte ad evitare che la prestazione, ivi compresa l'anamnesi, avvengano in condizioni di promiscuità
- garanzie di informativa ai soli terzi legittimati in ordine alle prestazioni eseguite e sulla dislocazione degli ospiti nell'ambito dei reparti, previo consenso degli interessati
- procedure atte a prevenire esplicite correlazioni fra l'interessato e reparti/strutture indicative di un particolare stato di salute
- tutela della dignità della persona, anche adottando – se del caso – accorgimenti provvisori per delimitare la visibilità dell'interessato durante l'orario di visita, ai soli familiari e conoscenti
- divieto di affissione di liste di ospiti/utenti in locali aperti al pubblico
- evitare la visibilità ad estranei di documenti sulle condizioni cliniche dell'interessato
- rilasciare informazioni sullo stato di salute a persone diverse dall'interessato solo dietro acquisizione di specifico consenso (anche rilasciato da persone legittimate a farlo in caso di impossibilità o incapacità dell'interessato) e solo per il tramite di un medico designato dall'interessato, o dal responsabile del trattamento dei dati (individuato – per i dati di carattere sanitario e per le cartelle cliniche - nel Direttore Medico e nel Direttore del Laboratorio di Analisi, per quanto di rispettiva competenza): quest'ultimo può autorizzare a ciò per iscritto operatori sanitari diversi dai medici che, nell'esercizio dei propri compiti, intrattengano rapporti diretti con i pazienti, individuando nell'atto di incarico appropriate modalità e cautele
- consentire il ritiro di referti diagnostici, risultati di analisi e certificazioni solo a terzi muniti di delega e con consegna in busta chiusa

D - TRATTAMENTO EFFETTUATO NELL'AMBITO DELLA FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI - TRATTAMENTO DI DATI MEDIANTE SISTEMA DOCUMENTALE ELETTRONICO

L'Azienda si avvale del sistema documentale Archiflow, che gestisce la protocollazione elettronica del documento, la assegnazione, lavorazione e archiviazione dello stesso in fascicoli elettronici. Come dichiarato dal fornitore, Archiflow garantisce un accesso ai dati, ai documenti e ai processi sicuro e controllato sia all'interno che all'esterno dell'organizzazione, anche in ottemperanza alle più recenti normative in materia di trattamento dei dati personali.
La protezione delle informazioni si basa su precise scelte a livello di architettura del sistema, che offrono una garanzia di protezione "fisica" del dato e a livello applicativo, che permettono di stabilire regole chiare di accesso alle informazioni in base all'identità degli utenti. Le caratteristiche funzionali di Archiflow consentono quindi di configurare il sistema in modo da garantire la compliance normativa.
Ai fini della gestione a norma della protezione dei dati, Archiflow attiva le funzionalità di profilazione degli utenti del sistema e dei loro diritti, di integrazione con i sistemi di autenticazione aziendali (Active directory; LDAP), di definizione delle regole di accesso e di visibilità dei documenti - anche a livello di singolo file - ai soli autorizzati, di registrazione delle operazioni effettuate, di possibilità di criptazione dei contenuti.

Per una corretta gestione del processo di trattamento è possibile attivare funzionalità utili a minimizzare la durata dello stesso, consentire la cancellazione, la rimozione o l'anonimizzazione dei dati (anche per specifico interessato), garantirne l'integrità.

Pertanto, vengono individuate – anche se del caso con il coinvolgimento del fornitore del sistema – le più opportune misure di compartimentazione di informazioni non ostensibili per intero alla più ampia platea di soggetti aziendali utilizzatori (meccanismi di limitazione della visibilità di copertine dei fascicoli, rubriche ed anagrafiche....) garantendone l'accessibilità ai soli soggetti coinvolti nella trattazione e/o destinatari dei dati per competenza, secondo principi di non eccedenza e pertinenza.
In particolare, si ha cura di adottare le seguenti cautele, necessarie ad evitare la conoscenza, anche accidentale, di informazioni a carattere riservato da parte di utenti che effettuassero ricerche generiche sul sistema:

- Creazione di fascicoli contenenti dati personali nell'oggetto classificandoli come limitati e condivisi con i soli servizi che devono averne la gestione;
- Riclassificazione della visibilità dei fascicoli già in uso contenenti dati sensibili da "Completa" a "Limitata", modificando il relativo flag nel Tab "Visibilità".
  Questa funzione permette di limitare la visibilità della copertina e l'accesso al Fascicolo ai soli uffici competenti o ai singoli utenti selezionati dall'organigramma POA, ed ha precipua rilevanza per gli ambiti che coinvolgono dati di carattere molto riservato (ospiti, inquilini, soggetti in contenzioso o con pendenze economiche nei confronti dell'Azienda, dipendenti, etc.);
- Limitazione della condivisione di schede documentali contenenti dati personali ai soli soggetti autorizzati alla trattazione secondo competenza e/o struttura di assegnazione.

E - TRATTAMENTO EFFETTUATO NELL'AMBITO DI PRESTAZIONE LAVORATIVA IN SMARTWORKING

Il Titolare del Trattamento deve adottare le misure tecniche e organizzative idonee a garantire la liceità e la sicurezza del trattamento dei dati, nonché la conformità dei trattamenti, anche in ordine alle attività svolte da remoto (e anche se il lavoratore utilizzi allo scopo strumenti propri), attraverso se necessario un innalzamento dei livelli di protezione, l'individuazione di nuove o diverse modalità di trattamento, l'emanazione di istruzioni appropriate.

Restano ferme le misure generali di cui alle precedenti lettere A e B, e inoltre:

a) Misure ed adempimenti in capo all'Azienda

a1 – misure tecniche

- Monitoraggio dei dispositivi di proprietà aziendale
- Implementazione di misure di sicurezza e modalità sicura di accesso da remoto; utilizzo di connessioni sicure (VPN o sistemi cloud based)
- Installazione e aggiornamento di sistemi di protezione antivirus e antispam e dei sistemi operativi

- Utilizzo di sistemi di back up offline
- Implementazione di adeguate procedure di gestione degli incidenti
- Individuazione di misure tecniche per assicurare la disconnessione del lavoratore e i tempi di riposo
- Adozione di politiche di back up automatizzato su server aziendale
- Adozione di crittografia (chiave asimmetrica) e tecniche di cifratura
- Definizione di processi di cancellazione sicura dei dati, smaltimento e distruzione
- Controllo degli accessi, definizione dei privilegi, rispetto del principio di minimizzazione del dato
- Regolamentazione dell'uso delle credenziali
- Utilizzo di sistemi di strong authentication (autenticazione a due fattori-2FA; processi di validazione basati sull'imputazione di ID e password personale con OTP)
- Adozione di sistemi di intrusion prevent
- Eventuale blocco di porte USB e connettori ad altre periferiche su device forniti
- Configurazione di pacchetto di applicativi autorizzati.

In ordine a quanto sopra, l'Azienda si è dotata di un "servizio di smart working sicuro", consistente in una macchina virtuale che pubblica in modo sicuro quanto presente sul server RDP Microsoft Remote Desktop creando di fatto un gateway utile a cifrare le comunicazioni fra il PC dello smart worker e la farm aziendale.

a2 – misure organizzative

- Effettuazione di attività di responsabilizzazione dei lavoratori
- Adozione di policy dedicate (indicazioni chiare su come utilizzare i dati al di fuori dell'Azienda, supporti consentiti etc.)
- Indicazioni sui trattamenti da effettuare, conferma della necessità di rispetto delle procedure di privacy, segreto e riservatezza, misure di sicurezza etc. già vigenti sul luogo di lavoro, etc.
- Divieto di modifica delle configurazioni autorizzate
- Divieto di installazione di software o applicativi non autorizzati
- Divieto di navigazione in siti non attinenti al rapporto di lavoro o non autorizzati
- Regolamentazione di condotte da adottare per l'operatività in contesti extradomestici
- Identificazione di un referente che il lavoratore da remoto possa contattare rapidamente in caso di dubbi e criticità

b) Adempimenti e cautele da richiedersi al lavoratore

- Sicurezza degli end point: aggiornare sempre il sistema operativo e l'antivirus, soprattutto in caso di utilizzo di dispositivi personali per scopi aziendali
- Corretto utilizzo dei device: se forniti dall'Azienda non devono essere utilizzati per scopi personali o famigliari, o promiscui; creazione di account personale in caso di strumento di proprietà condiviso; credenziali secretate
- Disconnessione dagli applicativi aziendali a fine sessione
- Controllo sulle reti domestiche (adeguatezza delle medesime)
- Adozione di cautele circa la postazione di lavoro nei confronti di congiunti, coinquilini, domestici, installatori, manutentori....anche con individuazione di locale ad hoc o altri accorgimenti di riservatezza
- Evitare il ricorso al vivavoce nelle comunicazioni, evitare possibili ascolti involontari o preterintenzionali
- Ubicazione della postazione di lavoro: al riparo da acqua, fonti di calore, animali domestici, conformità delle prese elettriche...
- Protezione fisica e custodia di device, documenti e supporti di memoria: conservazione in ambiente, armadio, cassetto, chiuso e ad uso esclusivo del lavoratore
- Cautele per linea internet e wi-fi: non utilizzare wi-fi altrui, hot spot pubblici o non conosciuti; credenziali adeguate per l'accesso alla rete domestica (non associabili alla persona); aggiornamento del firmer del router.

F - TRATTAMENTO EFFETTUATO NELL'AMBITO DEL WHISTLEBLOWING

Anche nel caso di whistleblowing, ovvero di segnalazioni volte a denunciare comportamenti connessi a possibile rischio corruttivo, o a violazioni del Modello Organizzativo ai sensi del D. Lgs. 231/01, l'acquisizione e la gestione della segnalazione danno luogo a "trattamento" per cui il Titolare ed i Responsabili del Trattamento (nel caso specifico, anche il RPCT e l'Organismo di Vigilanza – anche per il tramite della struttura di supporto) devono adempiere correttamente agli obblighi derivanti dalla disciplina di protezione dei dati personali; i trattamenti effettuati dai soggetti obbligati hanno come base giuridica e di liceità l'esecuzione di un compito di interesse pubblico tutelato dall'ordinamento, e sono necessari ad adempiere un obbligo legale cui è soggetto il titolare del trattamento.
Per il dettaglio delle attività circa la segnalazione di illeciti o comportamenti corruttivi, di gestione delle segnalazioni e per la tutela del segnalante si veda anche il vigente PTPCT.
Il trattamento viene effettuato anche per i dati connessi alle segnalazioni di infrazione del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01, ricadenti sotto la responsabilità e le competenze dell'Organismo di Vigilanza sul medesimo. Per le modalità di segnalazione, e le relative procedure, e le tutele connesse, si rimanda al MOGC vigente nel tempo e disponibile sul sito aziendale.

Per le segnalazioni che pervengono tramite il canale di posta ordinaria, a tutela del whistleblower restano ferme le misure generali di cui alle precedenti lettere A e B, e inoltre:

- occorre rispettare i principi di liceità, correttezza, trasparenza e minimizzazione dei dati
- i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

L'informativa agli interessati è resa disponibile alla totalità degli stessi mediante pubblicazione sul sito aziendale.

G - TRATTAMENTO EFFETTUATO NELL'AMBITO DELLA POSTA ELETTRONICA AZIENDALE

Il Titolare del Trattamento gestisce il trattamento dei dati personali del lavoratore relativi agli account di posta elettronica individualizzati (es. nome.cognome@azienda.it), per le finalità connesse all'espletamento del rapporto lavorativo. Per la tutela dei dati connessi alla e.mail aziendale si applicano le misure di sicurezza e le cautele di cui alla precedente lettera A), in quanto compatibili.

La gestione dell'account di posta aziendale da parte del Titolare è informata ai seguenti principi:

- l'account di posta aziendale non è uno strumento privato in uso esclusivo del lavoratore, ma uno strumento di lavoro di proprietà dell'Azienda. Di conseguenza, non c'è copertura della privacy quando il lavoratore utilizza l'e-mail aziendale per fini privati (ossia extra lavorativi), seppure autorizzati ad esempio in quanto considerati quale benefit
- in materia di verifica dell'account di posta aziendale del lavoratore, vige il generale divieto di controlli a distanza dei dipendenti, applicabile anche con riferimento al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica
- la prerogativa di effettuare controlli sull'account di posta elettronica del dipendente è peraltro consentita, legittima e proporzionata, quando sia necessario tutelare l'Azienda da eventuali comportamenti illeciti del dipendente (cosiddetti «controlli difensivi», destinati ad accertare un comportamento potenzialmente lesivo dell'immagine dell'azienda presso i terzi, o che possa comportare danni diversi per l'Azienda) e non anche per verificare l'esatto svolgimento della prestazione lavorativa. Ciò è possibile solo se il Titolare abbia già motivo di ritenere che sussistano tali condotte illecite (in pratica, è necessario che vi siano degli indizi di responsabilità a carico del dipendente: il controllo preventivo infatti è illegittimo). In ogni caso, il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento.
  Pertanto, le e-mail aziendali dei dipendenti sono suscettibili di controlli da parte del datore di lavoro, titolare del trattamento, che può così venire a conoscenza del contenuto della corrispondenza a queste condizioni:
    - a patto che il controllo non avvenga in forma generalizzata;
    - e che non serva come strumento di controllo della prestazione lavorativa;
    - il controllo deve avvenire per punire eventuali illeciti commessi dai dipendenti ai danni dell'azienda;

- il controllo non può mai essere preventivo ma deve essere supportato da indizi di responsabilità;
- sono vietati i controlli prolungati, costanti o indiscriminati o la raccolta a priori di tutte le e-mail dei dipendenti in vista di futuri ed eventuali contenziosi.

Il Garante per la Privacy giudica in contrasto con i principi di minimizzazione dei dati e di limitazione della conservazione la sistematica conservazione sul server aziendale per un esteso periodo di tempo di tutte le email inviate e ricevute dagli account aziendali, nonché di tutte le email presenti sull'account, in costanza del rapporto di lavoro o alla cessazione dello stesso, in vista di futuri possibili contenziosi o in relazione ad ipotetiche ipotesi di illeciti (o sospetto di commissione di illeciti) compiuti dal lavoratore.

In seguito alla cessazione del rapporto di lavoro del dipendente occorre che il Titolare (a) provveda alla rimozione previa disattivazione dell'account e alla contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi eventuali ultimi indirizzi alternativi riferiti alla attività professionale del cessato; (b) preveda che la disattivazione venga realizzata secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi su server aziendali.

L'inserimento della presente trattazione all'interno di questo Sistema di Gestione della Privacy – MOP – la cui conoscibilità è generalizzata - vale a tutti gli effetti a costituire informativa interna, diffusa a tutti gli interessati.

H - TRATTAMENTO EFFETTUATO NELL'AMBITO DEL SITO WEB ISTITUZIONALE E DEI SOCIAL MEDIA AZIENDALI

La consultazione e l'utilizzo del sito web istituzionale comportano il trattamento di dati dei fruitori, che necessita dell'adozione di talune cautele ai fini della migliore tutela.

- Dati di navigazione: queste informazioni non sono raccolte per essere associate a soggetti identificati, ma mediante l'associazione di altri dati potrebbero consentire l'identificazione degli utenti che si connettono al sito. Pertanto, occorre fissare termini di conservazione proporzionali alle singole finalità perseguite (ad es., elaborazione di statistiche anonime), e alla scadenza provvedere alla cancellazione o all'anonimizzazione degli stessi.
- Dati forniti volontariamente dall'utente: vengono inseriti per porre domande, fare richieste, compilare format, comunicare/interagire con l'Azienda. Particolare attenzione va posta all'inserimento di dati personali a tutela rinforzata (sanitari, giudiziari, etc.) nel corpo delle comunicazioni; ad esempio, nell'ambito di un servizio di prenotazione on line di prestazioni sanitarie, si richiamano in toto le indicazioni del Garante per la Privacy circa gli obblighi e gli adempimenti da rispettare
- Cookies: sono ammessi ai soli fini di acquisizione di dati statistici di accesso al sito, mantenere le preferenze dell'utente riguardo alla navigazione. L'uso di cookies persistenti è ammissibile unicamente se necessario alla resa di un servizio rientrante nei fini istituzionali dell'Azienda. Attraverso i banner l'utente ha la possibilità di stabilire e controllare le informazioni che intende fornire al sito

Il trattamento partecipa delle misure volte a garantire l'integrità e la riservatezza dei dati adottate dall'Azienda.

I - TRATTAMENTO DI DATI GIUDIZIARI

Si intendono per "dati giudiziari" quelli di cui all'art. 10 del GDPR, ovvero i dati "relativi a condanne penali, a reati o a connesse misure di sicurezza". Possono includersi anche i dati relativi all'applicazione di misure di prevenzione a seguito di provvedimento giudiziario.

Il trattamento dei dati giudiziari:

• è effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati proporzionate e necessarie in rapporto agli obblighi, ai compiti o alle finalità per i quali è autorizzato il trattamento;
• è limitato ai soli dati necessari per realizzare le finalità previste, sempre che le stesse non possano essere soddisfatte, caso per caso, mediante il trattamento di dati anonimizzati o di dati personali di natura diversa (principio di minimizzazione previsto nel GDPR);
• prevede l'obbligo di verificare periodicamente che i dati siano esatti, aggiornati, adeguati, pertinenti e necessari rispetto alle finalità del singolo caso;

• prevede l'obbligo di cancellazione dei dati nel caso in cui, anche a seguito delle verifiche, risultino non adeguati, non pertinenti o non necessari. È permessa l'eventuale conservazione, a norma di legge, dell'atto o del documento in cui sono contenuti.

Con riferimento all'Azienda, è consentito il trattamento dei dati giudiziari:

• per la gestione di rapporti di lavoro;
• per verificare e accertare requisiti di onorabilità;
• per tutelare diritti;
• per verificare la solidità, la solvibilità e l'affidabilità del contraente.

L - TRATTAMENTO DI DATI IN AMBITO URP

Gli sportelli URP presenti presso le sedi di lavoro, come pure l'Ufficio URP, garantiscono la massima riservatezza circa i dati personali contenuti nelle segnalazioni che agli stessi pervengono, tanto in relazione agli ospiti di riferimento, che in relazione ai dati relativi ai soggetti diversi che si rivolgono all'Ufficio.
Eventuali dati raccolti, rilevati o utilizzati nell'ambito della conduzione di indagini di customer satisfaction (qualora gli strumenti di indagine non prevedano già l'anonimato) non possono essere divulgati; gli esiti delle indagini vanno resi in forma anonima ed aggregata.
Segnalazioni, elogi, suggerimenti pervenuti dall'utenza possono essere esposti alle bacheche di reparto, ai fini della restituzione all'equipe o agli operatori interessati, avendo cura di oscurare tutti i dati (ivi compresi gli indirizzi mail del mittente) che possano direttamente o indirettamente ricondurre all'identità dei soggetti coinvolti.

§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§

I soggetti terzi che accedono alla struttura (compresi i volontari) devono rispettare, in materia di privacy e di approccio agli ospiti, tutte le regole e le garanzie previste per il personale. **In ogni caso, è previsto per i soggetti esterni il divieto di effettuare fotografie e/o riprese video di persone ed ambienti senza preventivo formale assenso rispettivamente da parte degli interessati e dei responsabili di struttura.**

§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§§

Gli incaricati del trattamento sono tenuti al rispetto delle misure di cui sopra, e per testare, verificare e valutare regolarmente l'efficacia delle medesime l'attuazione delle stesse è sottoposta a controlli a campione da parte del responsabile del trattamento o di soggetti tenuti a far rispettare le disposizioni di servizio.

8 - DOCUMENTI DI PRIVACY COMPLIANCE

Oltre al presente Modello Organizzativo – Sistema di Gestione, l'Azienda adotta ed implementa, in via non esaustiva, i documenti sotto indicati:

- Registro dei Trattamenti del titolare (RAT) -

tale documento indica le singole ATTIVITA' DI TRATTAMENTO, specificando per ciascuna quantomeno:

- Responsabilità sul trattamento dei dati
- Base giuridica del trattamento

- Finalità del trattamento
- Categorie di interessati
- Tipologia dei dati trattati
- Modalità di trattamento dei dati
- Tipologia delle operazioni eseguite
- Descrizione del trattamento e del flusso informativo
- Termini di cancellazione
- Descrizione generale delle misure di sicurezza tecniche e organizzative
- Categorie di destinatari per la comunicazione

Il Registro dei Trattamenti viene di norma revisionato almeno annualmente, e comunque in occasione di rilevanti variazioni dei trattamenti dei dati personali, e/o di variazioni dell'organizzazione interna, e/o delle norme vigenti in tema di protezione dei dati personali.

- Nomine dei Responsabili del trattamento
- Nomine degli incaricati del trattamento dei dati
- Valutazioni di impatto
- Registro delle violazioni (affidato per competenza alla struttura organizzativa deputata alla progettazione, attivazione e manutenzione del sistema di protezione dei dati, da implementare al bisogno)
- Informative sul trattamento, redatte secondo le indicazioni normative in materia.

Quanto sopra è integrato da documentazione di supporto relativa a specifiche attività di trattamento (es relazioni tecniche, valutazioni preliminari, autorizzazioni, circolari aziendali ed indicazioni ad hoc, ecc.). Rilevano in materia, altresì, le previsioni relative alla privacy ed alla gestione del trattamento dei dati contenute nel Piano Triennale per la Prevenzione della Corruzione e della Trasparenza ed Integrità, e nel Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001.

9 - INFORMAZIONE/FORMAZIONE DEGLI INCARICATI AL TRATTAMENTO

Gli incaricati al trattamento dei dati sono destinatari di istruzioni in ordine al trattamento dei dati, alle sue finalità, al controllo ed alla custodia degli atti e dei documenti contenenti dati personali, alla gestione in sicurezza delle banche dati e degli archivi di riferimento.
Vengono, inoltre, in particolare formati sui rischi relativi ai dati e sulle correlate misure di sicurezza, sugli accorgimenti operativi da adottare per la protezione degli stessi, sulle responsabilità derivanti dal processo di trattamento dei dati.
Tale formazione è prevista al momento dell'ingresso in servizio nell'unità operativa di riferimento dell'operatore destinato ad operazioni di trattamento dei dati, e – se del caso - in occasione di cambiamento di mansioni o di introduzione di nuovi strumenti o procedure rilevanti rispetto al trattamento dei dati personali. L'informazione e la formazione del caso sono effettuate e rendicontate direttamente dal responsabile della struttura organizzativa di assegnazione del dipendente, sulla base in particolare delle procedure operative, delle regole di buona condotta e delle indicazioni vigenti anche come riportate nel presente Sistema di gestione-modello di organizzazione.
Una formazione di carattere più generale riguardo alle norme in materia di tutela dei dati secondo le vigenti previsioni di carattere nazionale e sovranazionale viene prevista all'interno dei Piani di Formazione aziendale adottati annualmente.

10 - DIRITTO ALLA PROTEZIONE DEI DATI

Diritti dell'interessato
Ai sensi delle vigenti norme gli interessati possono esercitare, rispetto ai dati, i seguenti principali diritti:

- **Diritto di accesso**: l'interessato ha il diritto di ottenere dal titolare del trattamento conferma riguardo l'esistenza di trattamenti dei dati personali che lo riguardano, e in caso affermativo, di accedere ai dati personali e alle relative informazioni di trattamento (finalità, categorie di dati trattati, destinatari dei dati, periodo di conservazione, origine dei dati trattati, estremi identificativi di chi tratta i dati, esistenza di processi decisionali automatizzati/profilazione), anche per esercitare gli ulteriori diritti connessi.
  L'esercizio di tali diritti non deve recare danno ai diritti ed alle libertà altrui, o causare pregiudizi effettivi e concreti allo svolgimento di indagini difensive o all'esercizio di un diritto in sede giudiziaria.
- **Diritto di rettifica**: l'interessato ha il diritto di ottenere dal titolare del trattamento, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano, secondo il principio dell'esattezza del dato tenendo conto delle finalità del trattamento; l'Azienda adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati, anche verificando – quando necessario e per il tramite dei responsabili del Trattamento competenti - la correttezza, la coerenza e la corrispondenza al vero dei dati raccolti, se del caso confrontandoli con i dati appartenenti allo stesso interessato ma raccolti in momenti diversi o che abbiano una differente provenienza, rifiutando la raccolta dei dati incompleti o imprecisi, monitorando le operazioni di caricamento a sistema.
  L'Azienda provvede altresì all'eventuale aggiornamento dei dati direttamente forniti dal soggetto interessato dietro richiesta di quest'ultimo.
  L'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
- **Diritto di cancellazione/diritto all'oblio**: in particolare, gli interessati possano richiedere la cancellazione senza ingiustificato ritardo dei dati personali che li riguardano per i seguenti motivi:
  - perché i dati non sono più necessari per la finalità per i quali erano stati raccolti;
  - perché l'interessato ha revocato il consenso al trattamento dei dati;
  - perché l'interessato si oppone al trattamento;
  - perché i dati sono trattati illecitamente.

  Il genitore può richiedere la cancellazione dei dati personali del figlio minore o sul quale esercita la patria potestà.
  Le precedenti azioni non si applicano nella misura in cui il trattamento sia necessario:
  a) per l'esercizio del diritto alla libertà di espressione e di informazione;
  b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dall'Unione o dallo Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
  c) per motivi di interesse pubblico nel settore della pubblica sicurezza;
  d) per motivi di interesse pubblico, per finalità di ricerche storiche o scientifiche o ai fini statistici in quanto il diritto applicabile è suscettibile di rendere impossibile o seriamente compromettere il raggiungimento degli obiettivi di tale trattamento;
  e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
  Il diritto all'oblio si configura come diritto alla cancellazione in forma rafforzata, essendo previsto l'obbligo da parte del titolare che abbia pubblicato dati personali per i quali venga esercitato il diritto, di informare altri titolari che trattino i medesimi. L'interessato ha diritto di chiedere la cancellazione dei propri dati anche dopo revoca del consenso al trattamento.
- **Diritto di limitazione del trattamento**: in particolare, gli interessati possano richiedere la limitazione del trattamento dei dati personali che li riguardano per i seguenti motivi:
  - contestazione da parte dell'interessato dell'esattezza dei dati personali (limitazione per il periodo necessario al titolare del trattamento per verificare l'esattezza dei dati personali);
  - il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
  - sebbene il titolare non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - opposizione da parte dell'interessato al trattamento (limitazione in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato).

  Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
- **Diritto alla portabilità dei dati:** l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, quando il trattamento si basa sul consenso dell'interessato o sia necessario per l'esecuzione di un contratto a cui è soggetto l'interessato o per prendere provvedimenti su richiesta dell'interessato prima di stipulare un contratto. L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento ad un altro, laddove risulti essere tecnicamente

possibile. Il diritto alla portabilità dei dati non pregiudica il diritto di cancellazione. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di autorità pubbliche attribuite al titolare del trattamento.

- **Diritto di opposizione al trattamento:** L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
  Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o ai fini statistici, l'interessato ha il diritto di opporsi al trattamento, fatta eccezione se il trattamento è necessario per l'esecuzione di un compito di pubblico interesse.

- Inoltre, l'interessato può esercitare il **diritto all'oscuramento** dei dati all'interno del proprio Fascicolo Sanitario Elettronico al momento dell'erogazione della prestazione, prima dell'alimentazione del FSE, direttamente nei confronti del soggetto che la eroga, ovvero in qualunque momento successivo, tramite specifica istanza dell'assistito trasmessa al soggetto erogante. Nei casi in cui l'oscuramento di dati e documenti avviene successivamente all'alimentazione del FSE, le informazioni del dato o documento oscurato possono essere state utilizzate prima dell'oscuramento per la realizzazione di altri documenti, quali il Profilo sanitario sintetico, rispetto ai quali può autonomamente esercitare il medesimo diritto. Nel caso in cui sia stato esercitato il diritto all'oscuramento, l'assistito può revocare in ogni momento l'oscuramento di un dato o documento con le medesime modalità previste per l'esercizio del diritto di oscuramento. Nel caso di esercizio da parte dell'interessato del diritto all'oscuramento, i dati e i documenti oscurati potranno essere consultati esclusivamente dall'interessato e da chi abbia generato i predetti documenti.

Il titolare del trattamento comunica le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18 del Regolamento (UE) 2016/679, a ciascuno dei destinatari cui siano stati trasmessi i dati personali in questione tenendo conto della tecnologia disponibile e dei costi attuazione, e salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora lo stesso lo richieda.

Limitazioni e deroghe all'esercizio dei diritti

L'articolo 23 del GDPR consente agli Stati membri di limitare i diritti degli interessati, per diversi motivi tra cui la sicurezza nazionale e pubblica, per motivi di interesse generale e così via. Tali restrizioni devono rispettare l'essenza dei diritti e delle libertà fondamentali e devono essere a misura necessaria e proporzionata in una società democratica.
Tali limitazioni devono essere previste dalle disposizioni nazionali, quali le limitazioni e deroghe stabilire dal "Codice in materia di protezione dei dati personali", come segue:

art. 2-undecies: i diritti non possono essere esercitati con richiesta al titolare del trattamento, o con reclamo al Garante, qualora dall'esercizio dei medesimi possa derivare un pregiudizio effettivo e concreto:
a) agli interessi tutelati in materia di riciclaggio;
b) agli interessi tutelati in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) allo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
f) alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio
f-bis) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.
Tali diritti possono essere esercitati conformemente alle rispettive discipline di settore.

art. 2-duodecies: i diritti e gli obblighi relativi ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti avanti le autorità competenti sono disciplinati nei limiti e con le modalità previste dalle disposizioni che regolano tali procedimenti. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.

art. 3-terdecies: i diritti riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
L'esercizio di uno o più dei diritti non è consentito nei casi previsti dalla legge, o quando l'interessato lo abbia espressamente vietato con dichiarazione scritta, non equivoca, specifica, libera e informata, al titolare del trattamento.
In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte di terzi dei diritti patrimoniali che derivano dalla morte dell'interessato, nonché del diritto di difesa in giudizio dei propri interessi.

Inoltro delle richieste
L'interessato ad esercitare i diritti di cui sopra può inviare la propria richiesta:

I. scrivendo all'indirizzo di posta elettronica privacy@golgiredaelli.it,
II. scrivendo all'ASP Golgi-Redaelli – UOC Affari Generali - all'indirizzo di via Bartolomeo D'Alviano, 78 – 20146 Milano, tramite posta o con consegna diretta in loco all'Ufficio Protocollo.

Ai fini della evasione della richiesta occorre specificare i motivi della doglianza e le azioni ritenute necessarie (modifica, cancellazione,.....) e corredare la stessa con fotocopia del documento di identità del richiedente in corso di validità. Qualora la richiesta provenga da un soggetto terzo rispetto all'interessato, va altresì prodotta delega scritta da parte dell'interessato.
Nell'ipotesi in cui la richiesta fosse ricevuta da altri soggetti aziendali, sarà cura degli stessi comunicare all'interessato il corretto percorso, oppure inoltrare la richiesta in questione alla predetta UOC Affari Generali, senza per il momento dare altro o diverso seguito all'istanza, anche se afferente a trattamenti di competenza diretta.

Gestione delle richieste
A seguito della ricezione di richiesta da parte dell'interessato, la UOC Affari Generali la prende in carico e procede all'istruttoria relativa alla medesima, provvedendo in primo luogo alla verifica dell'identità del richiedente, della validità dell'istanza e dell'effettiva sussistenza del diritto dell'interessato, anche sulla base dei seguenti parametri:
• esistenza ed effettivo trattamento dei dati che riguardano l'interessato;
• contenuto dei dati che riguardano l'interessato (dati personali comuni, sensibili);
• valutazione dell'ampiezza della richiesta in relazione al diritto esercitato (proporzionalità).
Nei casi in cui la documentazione pervenuta non dovesse risultare adeguata, si richiedono all'interessato gli opportuni chiarimenti e/o l'integrazione della stessa con le informazioni mancanti. In caso di rifiuto da parte del richiedente, o di mancato inoltro di risposta in termini congrui e prefissati, si procede a rigettare la richiesta.
Le richieste da parte dell'interessato devono essere evase per iscritto (anche in caso di diniego) senza ingiustificato ritardo, e comunque entro il termine generale di 30 gg. dal ricevimento da parte della UOC Affari Generali. Detto termine si considera sospeso in caso di richiesta di chiarimenti, e riprende a decorrere dalla data in cui la UOC viene a conoscenza dei medesimi. Qualora dovessero verificarsi situazioni di particolare complessità, è possibile estendere fino ad un massimo di tre mesi le scadenze per l'evasione della richiesta dandone motivata notizia all'interessato.

Rilascio copie e richiesta contributi
Il titolare del trattamento su richiesta da parte dell'interessato deve fornire una copia dei dati personali oggetto di trattamento. Nel caso di richieste manifestamente infondate o eccessive, o ripetitive, o in cui l'interessato richieda più copie, si prevede un contributo spese ragionevole basato sui costi amministrativi, calcolato anche prendendo a riferimento eventuali tariffari adottati dall'Azienda per fattispecie analoghe.

11 - DPIA – VALUTAZIONE D'IMPATTO

Prima di effettuare trattamenti che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Regolamento richiede lo svolgimento di una valutazione d'impatto del trattamento sui diritti e sulle libertà dell'interessato (Data Protection Impact Assessment o DPIA), i cui risultati devono essere adeguatamente formalizzati.

Premesso che un singolo DPIA può esaminare un insieme di trattamenti simili che presentano rischi analoghi, l'istruttoria per la valutazione d'impatto deve essere effettuata:

- Identificando le possibili minacce alla sicurezza dei trattamenti;
- Considerando i requisiti di riservatezza, disponibilità e integrità dei dati personali;
- Considerando le necessarie misure di protezione tecnico-organizzativa da attuare per rendere il rischio accettabile.

Nel caso le misure ipotizzate siano ritenute adeguate (ovvero idonee a abbassare il livello di rischio fino a renderlo accettabile) il trattamento può essere effettuato.

La DPIA è richiesta, per quanto riguarda l'ASP Golgi-Redaelli, in particolare nei casi seguenti:

- trattamenti che comportano attività relative ad aspetti di salute dell'interessato
- trattamenti di dati avente carattere estremamente personale, connessi alla vita familiare e privata, e con impatto sulla vita quotidiana dell'interessato
- trattamenti non occasionali di dati relativi a soggetti vulnerabili
- Whistleblowing (ai sensi del D. Lgs. 24/2023)

L'Azienda, quindi, avuto riguardo alle proprie attività di trattamento, provvede senz'altro alla redazione ed all'aggiornamento di documenti di valutazione d'impatto in ordine a trattamento dei dati per ***Prestazioni di assistenza (sociale, sanitaria e socio-sanitaria), cura e tutela della salute - prestazioni accessorie di carattere alberghiero, ricreativo, assistenza religiosa - attività di studio e ricerca -** Soggetti interessati: Ospiti e utenti diversi degli Istituti geriatrici amministrati, parenti, familiari, care givers, amministratori di sostegno, curatori, tutori, * **Prestazioni legate a servizi riabilitativi dell'età evolutiva -** Soggetti interessati: Minori affetti da disturbi del comportamento e dello spettro autistico; parenti, familiari, care givers, amministratori di sostegno, curatori, tutori, ***Whistleblowers** – Soggetti interessati: Soggetti che effettuano segnalazioni volte a denunciare comportamenti connessi a un possibile rischio corruttivo, nonché a violazioni del Modello Organizzativo aziendale ex D. Lgs. 231/2001, e loro facilitatori (dipendenti dell'ASP, lavoratori autonomi e collaboratori, liberi professionisti e consulenti, lavoratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'ASP, volontari, tirocinanti, amministratori, colleghi, parenti o affetti stabili di chi ha segnalato). Soggetti segnalati. Altri soggetti coinvolti.

12 - DATA BREACH - VIOLAZIONE DELLA SICUREZZA DEI DATI

Nozione e cause

Per "*violazione della sicurezza dei dati personali*" si intende ogni evento che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati, e può assumere il carattere di:

- Violazione della riservatezza, in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione della disponibilità, in caso di perdita di accesso o distruzione di dati personali, anche a causa di eventi avversi;
- Violazione dell'integrità, in caso di alterazione non autorizzata o accidentale dei dati personali.

Le **cause** più comuni che portano ad un data breach si possono categorizzare in:

• Violazione involontaria ed accidentale: ad es. smarrimento di un supporto cartaceo, come un documento, o elettronico come un'unità flash USB, un palmare, un portatile;

• Furto: ad es, dei detti supporti cartacei e/o elettronici;

• Comportamento illecito da parte di dipendenti: ad es. violazione causata da un soggetto interno all'organizzazione, accedendo in maniera autorizzata alle informazioni, ma trattandole poi illegittimamente;

• Accesso non autorizzato/Alterazione dei dati: ad es. conduzione di un attacco avente come fine l'accesso senza autorizzazioni ai sistemi informatici, l'acquisizione dei dati personali e/o l'alterazione/divulgazione degli stessi;

• Impossibilità di accedere ai dati: per cause accidentali o per attacchi esterni (virus, malware....)

Segnalazione e gestione dell'evento dannoso

1. Chiunque venga a conoscenza di una effettiva o sospetta violazione della sicurezza dei dati personali, segnala immediatamente l'incidente al dirigente interessato.
2. Il dirigente:
   - prende in carico la segnalazione - informandone contestualmente il Titolare del Trattamento e il Responsabile della Protezione dei Dati - e conduce una valutazione iniziale dell'incidente per stabilire se si sia verificata una effettiva violazione della sicurezza dei dati personali, quando necessario avvalendosi dell'Amministratore di Sistema e/o di altri soggetti aziendali utili alla migliore definizione della problematica
   - in caso di accertata avvenuta violazione,
     - si occupa di acquisire, preservare, e documentare le evidenze e le analizza al fine di stabilire quantomeno:
     a. Quali dati personali sono coinvolti nella violazione
     b. La causa della violazione
     c. Come si è verificata la violazione
     d. L'entità della violazione (il numero di persone interessate)
     e. Le persone coinvolte nella violazione della sicurezza
     f. I dettagli delle informazioni, sistemi informatici, apparecchiature o dispositivi coinvolti nella violazione della sicurezza e qualsiasi informazione persa o compromessa a seguito dell'incidente.
     L'analisi è finalizzata anche all'individuazione di adeguate misure per arginare o eliminare l'intrusione e alla valutazione della necessità di attivare le procedure di comunicazione e di notifica
     - effettua la valutazione dei rischi correlati alla violazione, analizzando le conseguenze potenziali della violazione della sicurezza ed i possibili impatti sotto il profilo del rischio per i diritti e le libertà delle persone fisiche, e le probabilità di accadimento
     - evidenzia le azioni intraprese per risolvere la violazione, determina quali possibili ulteriori azioni correttive dovrebbero essere intraprese, sulla base del rapporto dell'incidente, per mitigare i rischi relativi alla violazione ed evitare che essa si ripresenti
   - a seguito delle analisi, informa il Titolare del Trattamento e il Responsabile della Protezione dei Dati, trasmettendo tutti i dati e le informazioni opportuni. Il Titolare e l'RPD vanno informati anche nel caso in cui l'istruttoria non evidenzi una violazione dei dati.

Notifica al Garante

Vanno notificate unicamente le violazioni che possono avere effetti avversi significativi causando danni fisici, materiali o immateriali agli interessati e comportando un rischio per i diritti e le libertà delle persone fisiche (ad esempio: la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità, il rischio di frode, la perdita di riservatezza di dati protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione, qualsiasi significativo svantaggio economico o sociale,....).

Il Titolare del Trattamento, valutata la necessità di attivare le procedure di comunicazione e di notifica anche con riferimento a quanto sopra sula base della situazione rappresentata dal Responsabile del Trattamento coinvolto, in caso affermativo notifica la violazione al Garante per la Protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. In caso di ritardo nella notifica, oltre il termine delle 72 ore, devono esserne giustificati i motivi.

La notifica al Garante deve essere effettuata tramite l'apposita procedura telematica disponibile sul portale dei servizi online dell'Autorità all'indirizzo https:/servizi.gpdp.it/databreach/s/ secondo i contenuti di cui al modello fac-simile presente alla stessa pagina.

Sul portale del Garante è parimenti disponibile uno strumento di self assessment utile per individuare le azioni da intraprendere in seguito ad una violazione dei dati personali derivante da in incidente di sicurezza.

Comunicazioni

Il Titolare del Trattamento nel caso in cui la violazione comporti un rischio **elevato** per i diritti e le libertà delle persone fisiche, come sopra, comunica obbligatoriamente la violazione a tutti gli interessati utilizzando i canali più idonei, a meno che siano già state poste in essere misure tali da ridurne l'impatto.

Contenimento e ripristino
Una volta accertato che si è verificata una violazione dei dati, l'Azienda deve intraprendere azioni immediate e appropriate per limitare la violazione.
Allo scopo, il Titolare del trattamento:
a. Valuta le eventuali azioni da intraprendere, proposte dal dirigente interessato a seguito delle analisi al fine di contenere l'incidente, mitigare i rischi, eradicare le eventuali minacce, e ripristinare la normale operatività
b. Qualora il dirigente non abbia già provveduto in tal senso, comunica agli attori coinvolti le misure da adottare al fine di contenere la violazione e coordina le attività
c. Emana le raccomandazioni per azioni future e miglioramenti nella protezione dei dati come rilevanti per l'incidente

13 - MONITORAGGIO E MIGLIORAMENTO DEL SISTEMA

L'efficacia e l'efficienza del Sistema di Gestione della Privacy sono soggette a verifica periodica (indicativamente annuale, e/o secondo necessità) in modo di assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e di favorire l'attivazione di un processo di aggiornamento continuo. La revisione deve verificare lo stato delle azioni preventive e correttive e l'aderenza alla politica privacy delle procedure in atto così come di quelle previste e non ancora applicate. Deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali, nonché dei risultati di precedenti riesami.
L'attività di controllo del sistema viene condotta principalmente prendendo in esame, quando presenti:

- I risultati della valutazione dei rischi
- I risultati delle valutazioni d'impatto
- Le registrazioni riferite alla violazione di dati personali
- Le segnalazioni di non conformità
- I reclami degli interessati e le azioni di esercizio dei diritti
- I nuovi pareri, linee-guida ed emanazioni del Garante
- I pareri e le opinioni delle parti interessate all'applicazione del sistema.

Il risultato dell'intero processo di revisione periodica include tutte le decisioni prese e le azioni adottate in merito al miglioramento del Sistema di Gestione della Privacy e se del caso può dare luogo ad un piano di miglioramento, che raccoglie le azioni da intraprendere, la relativa tempistica, l'impiego di risorse, i costi, le responsabilità e le altre valutazioni opportune allo scopo di risolvere eventuali criticità rilevate in fase di monitoraggio, affinché ne siano eliminate le cause e non se ne ripresentino le condizioni.